



Evaluating the Effectiveness of E-Learning within Cyber Security Education at the Secondary Level

Honours Project (Development) Final Report: MHG421879

P02274: BEng (Hons) Digital Security, Forensics & Ethical Hacking

Author: Tamar Everson

Email: tevers200@caledonian.ac.uk

Academic Year: 4th Year

Matriculation Number: S1226265

Project Supervisor: Katrin Hartmann

Second Marker: Frances Garven

Publication Date: 21st April 2017

Submitted for the Degree of
BEng (Hons) in Digital Security, Forensics and Ethical Hacking, 2016-2017

“Except where explicitly stated, all work in this report, including the appendices, is my own original work and has not been submitted elsewhere in fulfilment of the requirement of this or any other award”

Signed: _____

Date: _____

Abstract

There is a critical shortage of cyber security experts globally. Curriculums such as the Scottish Qualifications Authority (SQA)'s Cyber Security Fundamentals Unit are attempting to combat this shortage at the secondary school level, but teachers do not have the knowledge or resources to deliver these qualifications effectively. Research into delivering cyber security education via e-learning has been presented for higher education, but very little research has taken place which considers cyber security education at the secondary level. The cyber security e-learning solutions that currently exist are targeted at higher education, or those already in the industry.

This project uses the develop and test methodology to research the potential impact and suitability of delivering the SQA's cyber security curriculums via e-learning. An e-learning solution has been developed that attempts to enhance the overall cyber security learning experience in schools and helps teachers to deliver the cyber security qualifications more effectively. The developed system utilises a range of teaching methods to cater to each of the main types of learner. The e-learning application has been evaluated by both teachers and students in order to obtain a balanced and representative analysis. This analysis has shown that e-learning is an effective means of delivering cyber security education within secondary schools.

It is expected that the e-learning environment will improve the knowledge and understanding of cyber security in both students and teachers within secondary schools. The results from this project could increase the number of teachers delivering cyber security curriculums in schools, and help to bring more students into the cyber security industry by improving the quality of teaching they receive, thus reducing the cyber security skills deficit.

Acknowledgements

I would like to thank my supervisor, Katrin Hartmann, as well as all the other staff on the 7th floor, for their help and support throughout the project. I would also like to thank the staff at the Scottish Qualifications Authority, in particular Alistair MacGregor, Bobby Elliot, and Emma Campos, for their co-operation and willingness to give up their time to support this project. Additionally, Scott Hunter (Airdrie Academy), Andrew McGettrick (Strathclyde University), Kenneth Ovens (Glasgow Caledonian University) and the other school teachers and pupils with whom I have had contact with. Their help has been invaluable throughout the process.

My appreciation is also extended to all participants in my interviews and experiments, which gave me essential feedback on the evaluation of my application.

Finally, I wish to thank the regular faces in M704, my friends (including Carmen Metcalf, Anja Amundsen and Steven Ryland) and family for their support and understanding over the course of this academic year and throughout my studies.

Contents

1	Introduction.....	1
1.1	Background.....	1
1.1.1	The Current State of Cyber Security.....	1
1.1.2	Increasing the Number of Cyber Security Experts.....	1
1.1.3	E-Learning.....	2
1.1.4	Problem Summary & Solution.....	3
1.2	Project Outline and Research Question.....	3
1.2.1	Research Question.....	4
1.2.2	Aim and Objectives.....	4
1.2.2.1	Secondary Phase Objectives.....	4
1.2.2.2	Primary Phase Objectives.....	5
1.2.3	Hypotheses.....	7
1.2.4	Project Methodology.....	7
1.3	Report Structure.....	7
1.3.1	Literature Review.....	8
1.3.2	Problem and System Analysis.....	8
1.3.3	Design and Implementation.....	8
1.3.4	Testing and Evaluation.....	8
1.3.5	Discussions and Conclusions.....	8
1.3.6	Appendices.....	8
2	Literature Review.....	10
2.1	Evaluation of Existing E-learning Platforms.....	10
2.1.1	Codecademy.....	10
2.1.2	Khan Academy.....	11
2.1.3	Cybrary.....	13
2.1.4	Additional Reading.....	14
2.1.5	Conclusion.....	15
2.2	User Interface Design.....	15
2.3	Investigation of Common Learning Types.....	16
2.3.1	Visual Learners.....	17
2.3.2	Auditory Learners.....	17
2.3.3	Reading/Writing Learners.....	17

2.3.4	Kinaesthetic Learners.....	18
2.3.5	Conclusions.....	18
2.4	Investigation of the Teaching Material Needed.....	19
2.4.1	SQA Cyber Security Fundamentals Unit Specification.....	19
2.4.2	Unit Assessment.....	19
2.4.3	Required Teaching Materials.....	20
2.4.4	Conclusions.....	20
2.5	Methods of Collection and Analysis of Data.....	20
2.5.1	Qualitative Analysis.....	20
2.5.2	Quantitative Analysis.....	21
2.5.3	Heuristic Evaluation.....	21
2.5.4	Conclusions.....	21
2.6	Conclusions.....	22
3	Problem and Systems Analysis.....	23
3.1	Project Methods.....	23
3.1.1	Requirements Analysis.....	24
3.1.2	Design.....	24
3.1.2.1	Paper Prototypes.....	24
3.1.2.2	Final Designs.....	25
3.1.3	Implementation.....	25
3.1.3.1	Development Language.....	25
3.1.3.2	User Interface Framework: Bootstrap.....	26
3.1.3.3	Template Engine: Smarty.....	26
3.1.3.4	Style Management: Syntactically Awesome Style Sheets.....	26
3.1.3.5	MySQL.....	26
3.1.3.6	Development Integrated Development Environment & Software.....	26
3.1.3.7	GitHub.....	27
3.1.4	Deployment Testing.....	27
3.1.5	Evaluation.....	27
3.1.5.1	Staff Analysis.....	27
3.1.5.2	Schoolchildren Analysis.....	27
3.2	Lifecycle.....	28
3.3	Requirements Analysis.....	28
3.3.1	Interviews.....	30

3.3.1.1	Initial Interview with Teacher	30
3.3.1.2	Initial Interview with SQA	30
3.3.2	Literature.....	30
3.3.3	Identified Functional Requirements.....	30
3.3.4	Identified Non-Functional Requirements	31
3.3.5	Evaluation Participant Requirements.....	32
3.3.5.1	Student Participant Requirements	33
3.3.5.2	Staff Participation Requirements.....	33
3.4	Conclusions.....	33
4	Design and Implementation	34
4.1	Design	34
4.1.1	Initial Application Design Concepts.....	34
4.1.1.1	Initial User Interface Design.....	34
4.1.1.2	Final Database Structure.....	40
4.1.1.3	Final Navigation Structure.....	42
4.1.2	Teaching Material Design.....	43
4.1.2.1	SQA Learning Outcomes.....	43
4.1.2.2	Design of learning materials.....	44
4.1.2.3	Performance Criteria Targeted	44
4.2	Implementation	45
4.2.1	Application Development	45
4.2.1.1	Core Functionality	45
4.2.1.2	Access Control.....	45
4.2.1.3	User Assessment.....	46
4.2.1.4	System Security	47
4.2.1.5	System Maintainability.....	48
4.2.2	Teaching Material Development.....	48
4.2.2.1	Text Content	49
4.2.2.2	Image Content.....	50
4.2.2.3	Video Content.....	50
4.2.2.4	Audio Content.....	51
4.2.3	Final Application Design	51
4.2.4	Application Testing.....	52
4.2.4.1	Try Catch Blocks.....	52

4.2.4.2	Debugging Settings.....	53
4.2.4.3	Test Pages	55
4.2.4.4	Test Data.....	56
4.3	Deployment.....	56
5	Testing and Evaluation	58
5.1	Testing.....	58
5.1.1	Development and Post-Deployment Tests.....	58
5.1.2	As discussed in Section 4.2.3 Final Application Design	58
5.1.2.1	Debugging Settings.....	60
5.1.2.2	Test Pages	60
5.1.3	Test Cases	60
5.2	Evaluation	61
5.2.1	Student Evaluation	61
5.2.1.1	Methods	61
5.2.1.2	Results	62
5.2.1.3	Conclusions	65
5.2.2	Staff Evaluation	65
5.2.2.1	Methods	65
5.2.2.2	Results	66
5.3	Conclusions.....	68
6	Discussions and Conclusions.....	69
6.1	Project Summary.....	69
6.2	Final Discussion of Results.....	70
6.3	Project Limitations.....	71
6.4	Future Work	71
6.4.1	Gamification	71
6.4.2	Obtain a Larger Sample for Evaluation	72
6.4.3	Produce Additional Learning Resources	72
6.4.4	Expand Research to Evaluate NPAs In Cyber Security.....	72
6.4.5	Perform Detailed Analysis Against Learner Types	72
6.4.6	Conclusions.....	73
6.5	Project Conclusions	73
	Appendix A: References	I
	Appendix B: Nomenclature	XI

Appendix C: Related Resources	XII
Appendix D: Email and Interview Sources	XIV
D.1 Campos (2017).....	Error! Bookmark not defined.
D.2 Hunter (2016).....	Error! Bookmark not defined.
D.3 MacGregor & Elliot (2016).....	Error! Bookmark not defined.
D.4 McGettrick (2017).....	Error! Bookmark not defined.
Appendix E: Evaluation Forms.....	XXII
E.1 Staff Information Sheet & Consent Form.....	XXIII
E.2 Student Information Sheet & Consent Form	XXVI
E.3 Staff Worksheet	XXIX
E.4 Student Worksheet	XXX
E.5 Staff Questionnaire	XXXI
E.6 Student Questionnaire.....	XXXIV
Appendix F: Results.....	XXXVII
F.1 Student Evaluation Results	XXXVII
F.1.1 Question 1	XXXVII
F.1.2 Question 2	XXXVIII
F.1.3 Question 3	XXXVIII
F.1.4 Question 4	XXXIX
F.1.5 Question 5	XL
F.1.6 Question 6	XLI
F.1.7 Question 7	XLII
F.1.8 Question 8	XLIII
F.1.9 Question 9	XLIII
F.1.10 Question 10.....	XLIV
F.2 Student Quiz Results.....	XLIV
F.2.1 Questions.....	XLV
F.2.2 Question Scores	XLV
F.3 Staff Evaluation Results.....	XLVI
F.3.1 Question 1	XLVI
F.3.2 Question 2	XLVII
F.3.3 Question 3	XLVII
F.3.4 Question 4	XLVII

F.3.5	Question 5	XLVII
F.3.6	Question 6	XLVIII
F.3.7	Question 7	XLVIII
F.3.8	Question 8	XLVIII
F.3.9	Question 9	XLIX
F.3.10	Question 10	XLIX
Appendix G: Design & Functionality		L
G.1	Conceptual Design	L
G.1.1	Login	L
G.1.2	My Profile Page/Dashboard	L
G.1.3	Chapter List	LI
G.1.4	Chapter Introduction & Topic List Page	LII
G.1.5	Topic Page	LIII
G.1.6	Quiz	LIV
G.1.7	Quiz Results	LV
G.1.8	View Classes	LVI
G.1.9	View Students	LVII
G.1.10	Forgotten Password	LVII
G.1.11	Force Password Change	LVIII
G.2	Application Navigation	LIX
G.3	Database Schema	LXI
Appendix H: Project Architectural Design		LXIV
H.1	Navigational Structure	LXIV
H.2	Final Database Schema	LXV
Appendix I: Test Cases		LXVII
Appendix J: Test Data		LXIX
Appendix K: Source Code		LXXVIII
K.1	/	Error! Bookmark not defined.
K.1.1	/.htaccess	Error! Bookmark not defined.
K.1.2	/index.php	Error! Bookmark not defined.
K.1.3	/core/	Error! Bookmark not defined.
K.1.3.1	/core/.htaccess	Error! Bookmark not defined.
K.1.3.2	/core/class.chapters.php	Error! Bookmark not defined.
K.1.3.3	/core/class.classes.php	Error! Bookmark not defined.

K.1.3.4	/core/class.compare.php.....	Error! Bookmark not defined.
K.1.3.5	/core/class.core.php	Error! Bookmark not defined.
K.1.3.6	/core/class.database.php.....	Error! Bookmark not defined.
K.1.3.7	/core/class.email.php	Error! Bookmark not defined.
K.1.3.8	/core/class.encrypt.php	Error! Bookmark not defined.
K.1.3.9	/core/class.errorhandling.php.....	Error! Bookmark not defined.
K.1.3.10	/core/class.manipulate.php	Error! Bookmark not defined.
K.1.3.11	/core/class.pages.php	Error! Bookmark not defined.
K.1.3.12	/core/class.passwords.php	Error! Bookmark not defined.
K.1.3.13	/core/class.quiz.php	Error! Bookmark not defined.
K.1.3.14	/core/class.sanitise.php	Error! Bookmark not defined.
K.1.3.15	/core/class.schools.php	Error! Bookmark not defined.
K.1.3.16	/core/class.smartysetup.php.....	Error! Bookmark not defined.
K.1.3.17	/core/class.user.php	Error! Bookmark not defined.
K.1.3.18	/core/assets/	Error! Bookmark not defined.
6.5.1.2	/core/logs/	Error! Bookmark not defined.
K.1.4	/js/.....	Error! Bookmark not defined.
K.1.5	/pages/	Error! Bookmark not defined.
K.1.5.1	/pages/chapter.php	Error! Bookmark not defined.
K.1.5.2	/pages/dashboard.php	Error! Bookmark not defined.
K.1.5.3	/pages/forgotten-password.php.....	Error! Bookmark not defined.
K.1.5.4	/pages/login.php.....	Error! Bookmark not defined.
K.1.5.5	/pages/password-change.php.....	Error! Bookmark not defined.
K.1.5.6	/pages/view-classes.php.....	Error! Bookmark not defined.
K.1.5.7	/pages/view-grades.php	Error! Bookmark not defined.
K.1.5.8	/pages/view-users.php.....	Error! Bookmark not defined.
K.1.5.9	/pages/error-documents/	Error! Bookmark not defined.
K.1.6	/test/.....	Error! Bookmark not defined.
K.1.6.1	/test/test/chapters.php	Error! Bookmark not defined.
K.1.6.2	/test/test.classes.php.....	Error! Bookmark not defined.
K.1.6.3	/test/test.compare.php	Error! Bookmark not defined.
K.1.6.4	/test/test.core.php.....	Error! Bookmark not defined.
K.1.6.5	/test/test.database.php	Error! Bookmark not defined.
K.1.6.6	/test/test.email.php.....	Error! Bookmark not defined.

K.1.6.7	/test/test.passwords.php	Error! Bookmark not defined.
K.1.6.8	/test/test.schools.php	Error! Bookmark not defined.
K.1.7	/theme/.....	Error! Bookmark not defined.
K.1.7.1	/theme/default/	Error! Bookmark not defined.
K.2	SQL to create Database.....	Error! Bookmark not defined.

Table of Figures

Figure 2.a: Codecademy, a leading e-learning environment for programming	11
Figure 2.b: Khan Academy, free educational resources	12
Figure 2.c: Khan Academy progress view	13
Figure 2.d: Cybrary, free cyber security training.....	14
Figure 2.e: Types of learner	16
Figure 3.a: Project Development Process	24
Figure 3.b: Iterative Development (Microsoft, 2016b).....	28
Figure 3.c: Daily computer usage penetration of 16-24 year olds in Great Britain 2006-2015 (Statista, 2017b)	29
Figure 3.d: Frequency of computer use in the UK and EU in 2015 (Statista, 2017a)	29
Figure 4.a: Login Page.....	35
Figure 4.b: User Dashboard Design Concept	36
Figure 4.c: Chapter Introduction Design Concept	37
Figure 4.d: Topic Within Chapter Design Concept	38
Figure 4.e: My Classes View Design Concept	39
Figure 4.f: View Students View Design Concept.....	40
Figure 4.g: Final Database Schema	41
Figure 4.h: Unauthenticated User Navigation	42
Figure 4.i: Authenticated Student Navigation	42
Figure 4.j: Authenticated Teacher Navigation.....	43
Figure 4.k: Sample of Developed Teaching Materials	49
Figure 4.l: Sample of Developed Teaching Materials	50
Figure 4.m: Learning Material Page	51
Figure 4.n: View Grades Page	52
Figure 4.o: Sample Test Page	55
Figure 5.a: Bar Chart – Ease of Use of Application	63
Figure 5.b: Bar Chart – Learning Resource Preference	64
Figure 5.c: Comparison of Staff vs Student Views of Text-Based Resources	67
Figure 5.d: Comparison of Staff vs Student Views of Resources.....	67
Figure E.a: SQA Participant Information Form Page 1 of 2.....	XXIII
Figure E.b: SQA Participant Information Form Page 2 of 2	XXIV
Figure E.c: SQA Participant Consent Form.....	XXV
Figure E.d: Student Participant Information Form Page 1 of 2	XXVI
Figure E.e: Student Participant Information Form Page 2 of 2	XXVII
Figure E.f: Student Participant Consent Form.....	XXVIII

Figure E.g: Staff Questionnaire Page 1.....	XXXI
Figure E.h: Staff Questionnaire Page 2.....	XXXII
Figure E.i: Staff Questionnaire Page 3	XXXIII
Figure E.j: Student Questionnaire Page 1	XXXIV
Figure E.k: Student Questionnaire Page 2	XXXV
Figure E.l: Student Questionnaire Page 3	XXXVI
Figure F.a: Student Question 3 Results Bar Chart.....	XXXIX
Figure F.b: Student Question 4 Results Bar Chart.....	XL
Figure F.c: Student Question 6 Results.....	XLII
Figure G.a: Login Page	L
Figure G.b: User Profile Design Concept	LI
Figure G.c: Chapter List	LII
Figure G.d: Chapter Introduction & Topic List Design Concept	LIII
Figure G.e: Topic Within Chapter Design Concept.....	LIV
Figure G.f: Quiz Design Concept	LIV
Figure G.g: Quiz Results Design Concept.....	LV
Figure G.h: My Classes View Design Concept	LVI
Figure G.i: View Students View Design Concept	LVII
Figure G.j: Forgotten Password Design Concept	LVIII
Figure G.k: Password Change Design Concept.....	LVIII
Figure G.l: Unauthenticated User Navigation	LIX
Figure G.m: Student’s Navigation	LX
Figure G.n: Teacher’s Navigation.....	LX
Figure G.o: Database Scheme Image 1	LXII
Figure G.p: Database Schema Image 2.....	LXIII
Figure H.a: Unauthenticated User Navigation.....	LXIV
Figure H.b: Authenticated Student Navigation.....	LXIV
Figure H.c: Authenticated Teacher Navigation	LXV
Figure H.d: Final Database Schema.....	LXVI
Figure K.a: /theme/default/img/avatar.png.....	Error! Bookmark not defined.

Table of Tables

Table 2.a: Percentage of learner types based on VARK (2015) research.....	18
Table 4.a: Crow’s Foot Notation Key.....	41
Table 4.b: Quiz Question State	47
Table 4.c: Settings for Debugging Mode.....	54
Table 4.d: Bitwise Settings for Debugging Methods.....	54
Table 4.e: Server & Hosting Configuration.....	56
Table 5.a: Participant Scores.....	64
Table F.a: Student Question 1 Results.....	XXXVII
Table F.b: Student Question 2 Results.....	XXXVIII
Table F.c: Student Question 3 Results.....	XXXVIII
Table F.d: Student Question 4 Results.....	XXXIX

Table F.e: Student Question 5 Results	XL
Table F.f: Student Question 6 Results	XLI
Table F.g: Student Question 7 Results.....	XLII
Table F.h: Student Question 8 Results.....	XLIII
Table F.i: Student Question 9 Results	XLIV
Table F.j: Student Question 10 Results	XLIV
Table F.k: Quiz Questions	XLV
Table F.l: Participant Scores	XLV
Table F.m: Participant Quiz Scores	XLVI
Table F.n: Staff Question 1 Results	XLVII
Table F.o: Staff Question 3 Results	XLVII
Table F.p: Staff Question 4 Results	XLVII
Table F.q: Staff Question 5 Results	XLVIII
Table F.r: Staff Question 6 Results.....	XLVIII
Table F.s: Staff Question 7 Results.....	XLVIII
Table F.t: Staff Question 8 Results	XLVIII
Table F.u: Staff Question 9 Results	XLIX
Table F.v: Staff Question 10 Results	XLIX
Table H.a: Crow’s Foot Notation Key.....	LXV
Table J.a: Test User Data	LXIX

Table of Code Snippets

Code Snippet 1 : LoginRequired method of Core class.....	46
Code Snippet 2 : Video Display Code in /theme/default/templates/pages/chapter-page.tpl	50
Code Snippet 3 : Audio Embed Code in /theme/default/templates/pages/chapter-page.tpl	51
Code Snippet 4 : try catch block from User class.....	52
Code Snippet 5 : Debugging Settings within Core class	53
Code Snippet 6 : throwPHPError method of ErrorHandling class	53

1 Introduction

The following section introduces the current state of the cyber security industry, and what measures are being taken to improve cyber security education. The challenges faced in educating more cyber security professionals are also discussed before giving a detailed outline of the research project which has been undertaken.

The research question and project aims are outlined as well as the hypotheses which were formed at the start of this project. This is then followed by an outline of the structure of the remainder of this report.

1.1 Background

The following subsections provide an outline of the shortage of cyber security personnel, the actions being taken to combat the shortage, as well as the problem which this project aims to address.

1.1.1 The Current State of Cyber Security

This year (2017), there will be a shortage of two million cyber security experts worldwide (SQA, 2015a). According to Setalvad (2010), over 200,000 cyber security jobs in the US are unfilled. An e-skills UK (2013) report found that 85% of companies surveyed struggle to recruit enough cyber security candidates. This equates to only ten to fifteen percent of information security vacancies being filled. IT roles have climbed into the Top 10 hardest jobs to fill as per the ManpowerGroup 2015 Talent Shortage Survey (ManpowerGroup, 2015). As these figures show, the shortage of trained people within cyber security is at a critical level. As such, work needs to be undertaken to improve the uptake of careers in cyber security.

1.1.2 Increasing the Number of Cyber Security Experts

Governments around the world are now beginning to realise that something needs to be done to increase the number of people within the industry, and to help protect against the cyber threat (Evans & Reeder, 2010). The EU is extremely concerned about cyber security, and are in ongoing discussions on the topic (McGettrick, 2017)¹. A number of higher education courses for cyber security have been launched in recent years, including at both Glasgow Caledonian University and Abertay University in Scotland. These higher education courses will help to alleviate the shortage. Many experts such as Jeffrey Carpenter believe that the best way to achieve the goal of reducing the cyber security skills shortage is through education from the secondary school level (Mohoney, 2011).

The UK Government has taken a number of measures since 2011 to improve the nation's cyber security capability, as outlined in The UK Cyber Security Strategy 2011-2016. These include the introduction of cyber security within GCSE computer science, and through higher education initiatives (Cabinet Office, 2016). In 2010, the Cyber Security Challenge UK was established

¹ The full email trail with McGettrick can be found in Appendix **Error! Reference source not found. Error! Reference source not found.**

(Cyber Security Challenge, 2016a), and has made a strong impact on cyber education within the United Kingdom (Everson, 2016; Nowill, 2014). The Cyber Security Challenge’s education programme uses a mix of virtual and face-to-face learning methods (Cyber Security Challenge, 2016b).

Additionally, in 2015, the Scottish Qualifications Authority (SQA) announced that it was working with industry and educators to create a number of cyber security courses, including the Cyber Security Fundamentals Unit and some National Progression Awards (NPAs) in cyber security to “help our young people to develop the skills and knowledge they need to be safe online” (Robertson, 2015). The aims of the qualifications are to inform students of the rights and responsibilities of everyone who uses the internet and computer resources (SQA, 2015d), as well as to help to combat the shortage of cyber security professionals. The qualifications are now being taught in schools across Scotland, and the cyber security NPAs are thought to become one of the most popular NPAs within the next few years.

1.1.3 E-Learning

The Oxford English Dictionary defines e-learning as “Learning conducted via electronic media, typically on the Internet” (Stevenson, 2015). E-learning is widely used at the higher education level, with many universities using applications such as Blackboard² or Moodle², and some even moving to deliver courses entirely online through Massive Open Online Courses (MOOCs). As González (2010) says, e-learning is becoming a part of the normal on-campus education system within universities as well as for distance education.

Despite the wide adoption of e-learning in higher education, “ELearning at the secondary level is an emerging concept” (Henley, 2009). Scotland’s secondary education system is ahead of many other countries with their e-learning capabilities, with the utilisation of the Glow Connect e-learning platform. At the time of launch, Glow Connect was thought to be the largest e-learning platform in the world (Davitt, 2006). Since Henley’s paper, tools such as BBC Bitesize² and the aforementioned Glow Connect² have started to be adopted in secondary schools as a method of e-learning for students. The BBC’s Bitesize is an excellent resource aiding in the revision and learning of a number of key curriculum subjects (Turner, 2003).

At the time of undertaking this research, BBC Bitesize does not provide resources for either the Cyber Security Fundamentals curriculum or the NPAs in Cyber Security, with the most relevant content being the BBC’s Computer Science resources. Glow Connect (formerly Scottish Schools Digital Network) was launched in 2007 (Walker, 2007; Davitt, 2006), and is used in schools throughout Scotland. It does not provide sufficient capabilities to allow a full e-learning environment for the NPAs in Cyber Security. A number of other online resources exist for computer programming, such as Codecademy² and Code School², but these do not cater for the SQA’s cyber security qualifications.

² Links to all external resources mentioned throughout this report are available in Appendix C: Related Resources

A number of security-focussed e-learning platforms do currently exist, but these target people already in the IT industry (Chen & Tao, 2012) or higher education students, rather than school pupils. Chen and Tao's (2012) SWEET environment³ provides a number of practical exercises that can be undertaken in the computer lab. These lab exercises are in the form of a self-contained virtual machine that can be downloaded and run by the student. Additionally, the SEED environment³ uses a similar framework, with a number of lab exercises provided in a downloadable virtual machine (Du & Wang, 2008). These existing environments attempt to make cyber security education more accessible, but do not cater to the secondary school level.

1.1.4 Problem Summary & Solution

The one major problem with the new cyber security qualifications offered by the SQA is that school teachers do not have sufficient Information and Communications Technology (ICT) skills (Fernández-Cruz & Fernández-Díaz, 2016) to effectively deliver curriculums in cyber security. In order to encourage more people into the cyber security industry, teachers need the resources to aid them in teaching these new units.

Dewey (1963) points out that experience arouses curiosity and pushes people to learn more. This is still true today, with students far more likely to effectively learn subjects such as cyber security through active learning techniques than through entirely theory-based learning. Different people learn in different ways, and it is important that any new resources, which are designed to aid in the teaching of the cyber security curriculums, consider this fact. The four main types of learner are Visual, Auditory, Reading/Writing, and Kinaesthetic learners (Ebert & Culyer, 2013, p.79). E-learning is a good method of teaching as it can easily be developed in a way to effectively cater towards these four main types of learner.

Current teaching materials for both the Scottish NPAs in Cyber Security and the Cyber Security Fundamentals unit are insufficient for teachers to effectively deliver the courses to their students. More resources need to be developed in order to enhance the education secondary level students receive in cyber security, and to enable more teachers to deliver the qualifications. Due to its ability to cater to the four main learner types, an e-learning environment is likely to have a wide, and positive, impact on students and teachers when learning the cyber security curriculums.

1.2 Project Outline and Research Question

The work carried out in this project has developed an e-learning platform to deliver the SQA's Cyber Security Fundamentals programme, and seeks to determine the effectiveness of this e-learning solution in improving the overall quality of education that students receive for this curriculum. The project aims to develop a comprehensive e-learning platform that will cater to the four main types of learner, and help to engage students through the process of completing the cyber security curriculum in schools. Upon completion of the development of the application, research participants were asked to evaluate the effectiveness of the solution.

³ Links to all external resources mentioned throughout this report are available in Appendix C: Related Resources

1.2.1 Research Question

The research question has been formulated to focus on the lack of teaching resources for cyber security education in schools, and aims to focus the project on the effectiveness of e-learning to successfully mitigate this lack of resources. The question is stated below:

“Would the development of an e-learning environment for the SQA’s Cyber Security Fundamentals unit improve students’ understanding of cyber security and increase their abilities in the subject?”

The aims and objectives of the project are outlined in the following section. The aims were formed in order to focus the project on answering the research question posed above.

1.2.2 Aim and Objectives

The primary aim of this project was to investigate and evaluate the effectiveness and suitability of online virtual learning in a cyber security setting. This has been achieved by developing an e-learning system to teach the SQA’s Cyber Security Fundamentals unit. This has been investigated by devising a user experiment where users performed a series of tasks using the application. The users then answered a questionnaire based on their experience. Members of teaching staff and SQA representatives have also been interviewed.

A number of primary and secondary phase research objectives have been identified in order to effectively assess the effectiveness of online virtual learning in a cyber security setting. The following subsections outline these objectives.

1.2.2.1 Secondary Phase Objectives

The objectives outlined in this section have been met by reading relevant literature surrounding e-learning and cyber security education. The secondary objectives have been researched in preparation for this report, and are discussed in further detail in Section 1.2.2.1 Secondary Phase Objectives.

SO1: Evaluate existing e-learning platforms and literature to identify what works well and what does not work well with the design and content structures

By evaluating what does and does not work well within existing e-learning platforms, a detailed development plan was established. This allowed functional and non-functional requirements for the successful e-learning environment to be specified, allowing development time to focus on the aspects that are likely to make an e-learning environment succeed for cyber security education. These requirements are outlined in Sections 3.3.3 Identified Functional Requirements and 3.3.4 Identified Non-Functional Requirements.

SO2: Identify the most common learning types to determine an effective way to deliver e-content

As discussed by Ebert & Culyer (2013, p.79), there are four main types of learners. By identifying methods of effectively teaching students of each learning type, consideration has been given during the development of the e-learning system to cater to these. The process of developing the learning materials is outlined in Section 4.1.2 Teaching Material Design.

SO3: *Identify the learning resources which need to be included in an online learning environment for the SQA's Cyber Security Fundamentals unit*

In order to successfully deliver cyber security education in schools via an e-learning environment, careful consideration has been given to the curriculum. By analysing the Cyber Security Fundamentals curriculum, the provided resources have been tailored to suit the students' learning needs. It should be noted that the SQA curriculum is very limited in its communication of the standard of knowledge which students should have upon completion of the units.

SO4: *Research Methods of Collecting and Analysing Data*

The effectiveness of the e-learning environment for delivering cyber security education was evaluated by using a combination of evaluation methods. Research has been undertaken to determine the methods that should be used.

1.2.2.2 Primary Phase Objectives

The objectives outlined in this section have been met by using primary research methods. Sections 3 to 5 discuss each of these objectives in further detail.

PO1: *Develop a prototype e-learning environment to deliver cyber security training*

A Prototype e-learning environment has been developed to host the training materials which were developed in PO2. The environment allows for the management of students and enables teachers to view students' progress.

PO2: *Develop learning materials for use in the e-learning environment*

Training materials utilising a range of media types were developed to suit each type of learner. Resources have also been produced to assist with the learning and assessment process. The development of the learning materials is outlined in Section 4.1.2 Teaching Material Design. The materials have then been evaluated through PO3-PO6.

PO3: *Formulate a questionnaire for users of the e-learning environment*

A questionnaire was developed for both staff and students to complete based on their usage of the e-learning environment (PO4 and PO5). The questions used a mixed method of research, as discussed in Section 3.1.5 Evaluation, and results have been anonymised for the final report. Conclusions have been drawn based from the questionnaire results, as discussed in PO7. The use of a questionnaire is a resource friendly method of obtaining a data set on several elements of the e-learning environment.

PO4: *Develop a user experiment to test the effectiveness of the e-learning environment*

A user experiment has been developed in order to get research participants to use specific aspects of the e-learning environment. This helps to obtain data about what real users find effective or ineffective with the application. The usage of the application, as well as the results from the questionnaire in PO3, have helped to draw conclusions as to the effectiveness of the environment in aiding cyber security education in schools. The process of formulating the experiment is further discussed in Section 3.1.5 Evaluation.

PO5: *Source a sufficient set of appropriate users for the experimentation phase of the project by contacting the SQA, schools, colleges, and Education Scotland*

A suitable set of participants were needed in order to evaluate the environment. The participants were a mix of students and teaching staff, as each user group has different needs and requirements. Details of how the users were sourced are given in Section 3.3.5 Evaluation Participant Requirements.

PO6: *Execute the user experiment using the questionnaire and experiment to test the e-learning environment*

Both the user experiment devised in PO4, and the questionnaire formulated in PO3 were given to the subjects from PO5. The subjects were asked to complete the user experiment and questionnaire in order to gather data which could be analysed in PO7 to determine the effectiveness of the solution in delivering secondary school level cyber security curriculums.

PO7: *Analyse the results from the human experimentation phase to determine the outcome of the project and draw conclusions on whether the hypothesis posed in the research question is true*

The data gathered in PO6 was analysed to determine information regarding the effectiveness of e-learning within secondary level cyber security curriculums. These results are discussed in Section 5.2 Evaluation.

1.2.3 Hypotheses

By developing an e-learning environment for the Cyber Security Fundamentals unit, hypotheses were developed based on the expected outcomes of this project. Relevant literature has been discussed to provide justification for each hypothesis. Section 6 Discussions and Conclusions discusses the validity of these hypotheses based on the research findings.

Hyp1: The developed online resource will help students to further their learning of the Cyber Security Curriculum.

Liaw *et al.* (2007) found that the majority of computing students who used an e-learning system for a module in college found e-learning to be effective and improved a range of skills. Additionally, most instructors perceived e-learning to be an enjoyable and useful way for students to learn.

Hyp2: The resulting online resource will help teachers to better deliver the Scottish Cyber Security Curriculum.

Liaw *et al.*'s (2007) research found that most instructors surveyed intend to use e-learning technologies for their teaching. The research also found that instructors believe e-learning to be very useful for both learning and teaching.

1.2.4 Project Methodology

This project uses the “Develop and Test” methodology in order to investigate the research question outlined in Section 1.2.1 Research Question. During interviews with the author, both Hunter (2016)⁴ and MacGregor & Elliot (2016)⁵ explained the shortage of resources available to aid teachers in the delivery of the SQA’s cyber security curriculums. As such, an e-learning environment needed to be developed to answer the research question. Section 3.1 Project Methods provides further detail on the methods used within the project.

1.3 Report Structure

The structure of the remainder of this report is outlined in the following subsections. The content of the literature review, problem and system analysis, design and implementation, testing and evaluation, and discussions and conclusions are briefly discussed.

⁴ Details of the interview with Hunter can be found in Appendix **Error! Reference source not found. Error! Reference source not found.**

⁵ Details of the interview with MacGregor & Elliot can be found in Appendix **Error! Reference source not found. Error! Reference source not found.**

1.3.1 Literature Review

Section two of this report consists of a detailed literature review on a number of topics which are relevant to this project. It outlines existing e-learning platforms, common learning techniques, the teaching materials which need to be provided to deliver the SQA curriculum, as well as methods of data collection and user interface design.

Each section of the literature review corresponds to one of the project objectives. Each area mentioned above has been explored, analysed, and presented with conclusions drawn by the author.

1.3.2 Problem and System Analysis

Section three of this report details the problem which the author identified during initial research, as well as a discussion of the requirements of the system which has been developed. It provides a general overview of the main stages which have been completed throughout the project, as well as describing detail relating to the development process, including the development lifecycle and the functional and non-functional requirements of the system.

The use of the develop and test methodology is discussed and justified, as well as analysis of various possible solutions and detail of the methods used to research these solutions.

1.3.3 Design and Implementation

Section four of this report provides an explanation of the key design aspects of the developed system. This includes the user interface design, database design, design of the teaching materials and evaluation design. The initial designs of the various sections of the project are discussed, followed by an outline of the final design solution. This section justifies each of the elements of the design process.

1.3.4 Testing and Evaluation

Section five of this report details the evaluation methods used to test the hypotheses proposed in Section 1.2.3 Hypotheses. Both students and teaching staff were asked to use the e-learning environment and fill in a subsequent survey based on their usage of the application. The full results from the evaluation are available in Appendix F: Results.

1.3.5 Discussions and Conclusions

Section six brings the report to a conclusion. It summarises the project and provides discussion around the results of the evaluation in relation to both the research question and hypotheses. This section also outlines the project's limitations and areas where future work could be undertaken to build on the research produced in this report.

1.3.6 Appendices

The appendices detail any supporting material which is referenced throughout the report. The appendices are available as a separate physical document to the main report due to their length. The appendices are structured as detailed below.

Appendix A contains the list of references used throughout this project, formatted in GCU Harvard style referencing. There is a total of 111 references listed within Appendix A.

Appendix B is a nomenclature detailing the definitions of the abbreviations used throughout this document.

Appendix C details resources related to this project, including links to the e-learning platforms discussed within the literature review.

Appendix D details the emails between the author and experts, as well as interviews which the author has conducted as part of this research project.

Appendix E contains the documentation which was provided to participants in the evaluations prior to, and during, the evaluation phase. This includes the parental consent forms for student participants and the worksheets that participants had to work through. It also includes the questionnaires that participants completed.

Appendix F contains the full results from each of the three evaluation phases. This includes the student evaluation results, the student quiz results, and the teacher evaluation results.

Appendix G outlines information regarding the design and functionality of the e-learning environment, including conceptual designs of the application's navigation and page designs.

Appendix H outlines the application's final architectural design, including the database schema and navigational structure.

Appendix I details the test cases used by the author when evaluating the e-learning system during the functional testing phase of development and implementation. This took place prior to the staff and student evaluations taking place.

Appendix J lists the test user accounts which were created in order to test the application.

Appendix K contains all of the source code for the application including the PHP code, and the SQL needed to create the empty SQL Database that the application runs on.

2 Literature Review

The literature review aims to address and complete the secondary objectives set out in Section 1.2.2.1 Secondary Phase Objectives, which are reiterated below for references:

- SO1: *Evaluate existing e-learning platforms and literature to identify what works well and what does not work well with the design and content structures*
- SO2: *Identify the most common learning types to determine an effective way to deliver e-content*
- SO3: *Identify the learning resources which need to be included in an online learning environment for the SQA's Cyber Security Fundamentals unit*
- SO4: *Research Methods of Collecting and Analysing Data*

By gaining an in-depth knowledge of these objectives, a more effective e-learning environment can be developed in order to improve the quality of the research and answer the research question posed in Section 1.2.1 Research Question.

Upon completion of secondary objective SO1, the author concluded that additional literature review should be undertaken to identify methods user interface design. As such, information on this topic is also provided in the following sections.

2.1 Evaluation of Existing E-learning Platforms

A large number of e-learning platforms currently exist to teach students a variety of subjects. Three of these have been investigated by reviewing relevant literature and spending time using the e-learning platforms. The following sub-sections discuss each platform.

There is very little literature available evaluating existing e-learning platforms. As such, this section mainly focuses on the author's own experiences of evaluating the platforms with literature cited within the discussions wherever possible.

2.1.1 Codecademy

Codecademy (see Figure 2.a) is an interactive online learning environment which lets students learn to code for free (Codecademy, 2017). It allows teachers to login and manage classes. A range of people and organisations use Codecademy to both learn and teach, including secondary schools and colleges (Ma, 2013). New York University joined forces with Codecademy in 2012 to run a successful programming module (Finley, 2012).

Research by Lee and Ko (2015) found that Codecademy's method of teaching in a tutorial style is more effective than other learning styles such as games at teaching programming. Based on this research, it is considered likely that a similar approach towards teaching cyber security is likely to enhance the cyber security learning experience more than some of the other methods such as games which are discussed in Lee and Ko's research.

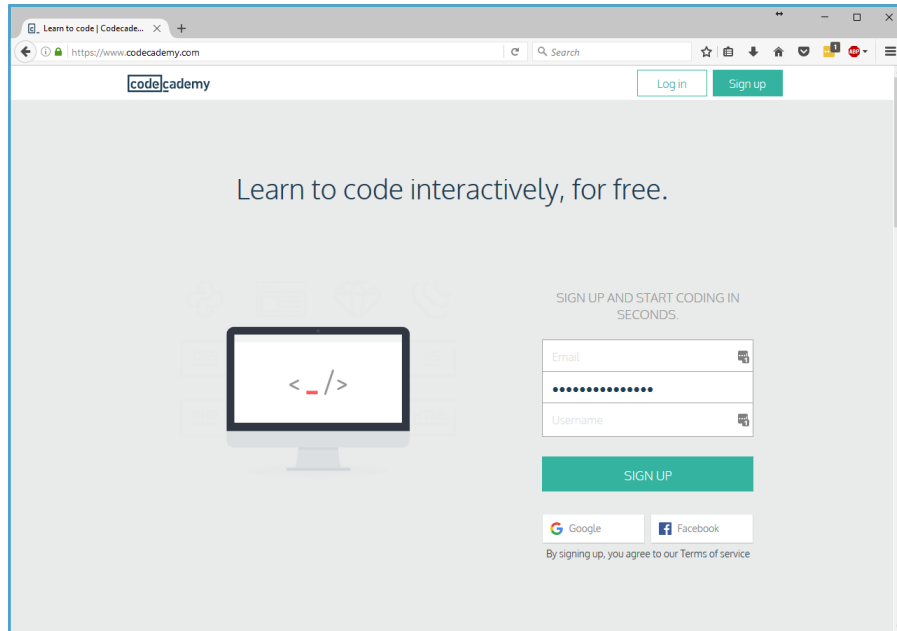


Figure 2.a: Codecademy, a leading e-learning environment for programming

Codecademy offers a variety of incentives to encourage users to learn through the platform. Users gain points as they progress through each course, as well as achieving badges for achievements such as completing a number of exercises, or learning a key concept. The use of points systems makes students more competitive and encourages participation and learning by publically displaying leader boards (Olsson & Mozelius, 2016). The use of systems such as this in learning is referred to as gamification, which is “the use of game design elements in non-game contexts” (Deterding *et al.*, 2011).

Codecademy has a clean and easily navigable user interface (UI), making it easy for users to flow through the learning modules and select the topics that they wish to learn. Because of the UI design, users are not hindered in their learning experience, but instead they are naturally encouraged to continue with their learning. This can lead users to want to undertake the learning for its own sake without considering the fact that they are learning from the experience of using the e-learning platform (Johnson & Wiles, 2003).

Codecademy is a very popular e-learning environment for learning programming on, but does not offer other subjects such as cyber security education or general computing. Some of the techniques used by Codecademy to engage users in programming should, however, be transferrable to other subjects such as cyber security.

2.1.2 Khan Academy

Khan Academy (see figure Figure 2.b) “offers practice exercises, instructional videos, and a personalized learning dashboard” (Khan Academy, 2017) which allows students to learn a variety of subjects including maths, computing and economics online free of charge. Khan Academy includes some cryptography content within its computer science resources, but does not offer a cyber security specific curriculum.

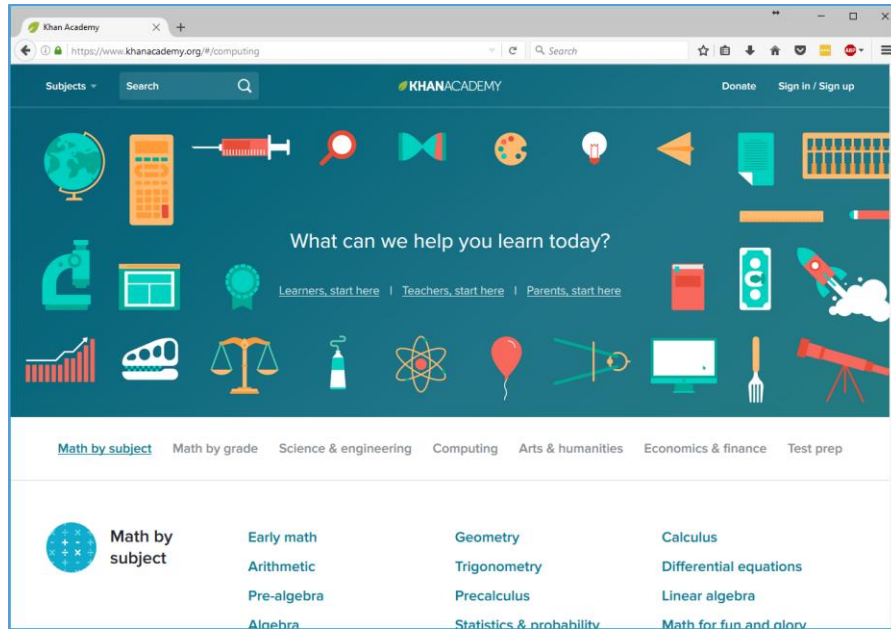


Figure 2.b: Khan Academy, free educational resources

Khan Academy has a range of features to help both students and educators using the environment, including a progress section that both students and their teachers can access. This shows both students and teachers how far through the different sections the student is, as well as which areas the student needs more practice or help with, as shown in Figure 2.c.

Khan Academy has taken a number of approaches to engage users by leveraging their “natural desires to compete and obtain achievements” (Morrison & DiSalvo, 2014). These methods allow users to gain a sense of achievement upon completing each task within the e-learning environment, which encourages them to continue learning.

Morrison & DiSalvo (2014) discuss a number of the approaches that Khan Academy uses to create a gamified experience in detail. Just like Codecademy, students can earn points and badges as they complete “missions”. This helps to engage the students. The system also suggests specific goals that users should attempt to complete, utilising students’ motivation to complete challenges that they are presented with.

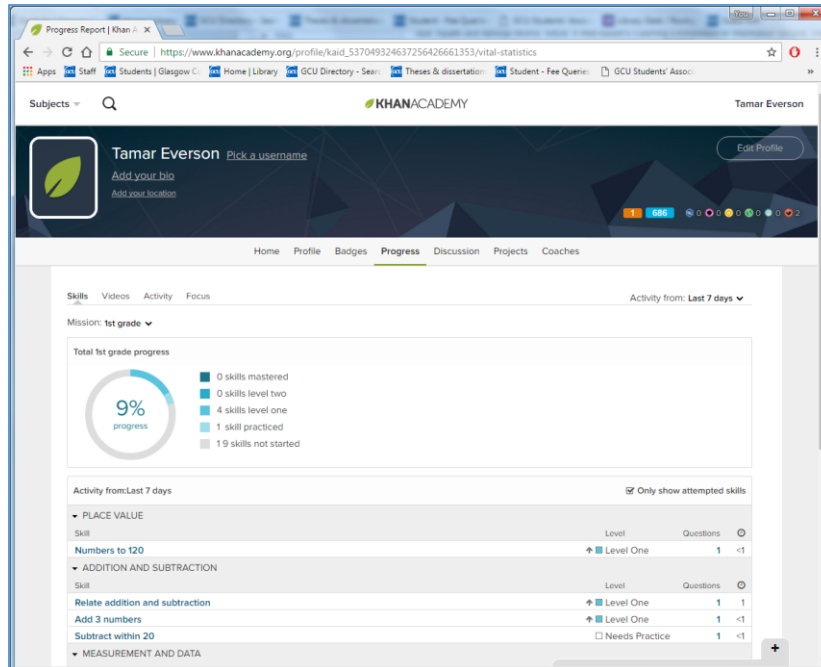


Figure 2.c: Khan Academy progress view

The UI within Khan Academy is not as easy to use as Codecademy, but still actively encourages users to continue with their learning. Cho *et al.* (2009) explain that a key factor in encouraging continued usage of an e-learning system is perceived user interface design. If the application is relatively intuitive and easy to use, people are more likely to continue using it than if it is cumbersome to use. There are aspects of Khan academy that have been considered in terms of UI, and aspects that the author avoided when developing the cyber security e-learning system.

As with Codecademy, Khan Academy mainly focuses on getting the students to actively take part in activities. This is in contrast to Cybrary, which is discussed in the following section. As such, Khan academy is suited towards kinaesthetic learners more whereas Cybrary is more tailored towards visual and auditory learners.

2.1.3 Cybrary

Cybrary (see figure Figure 2.d) provides free cyber security training around a range of topics and security qualifications. Content is delivered through videos, and there is a supporting user forum. Cybrary (2016; Cybersecurity Excellence Awards, 2016) won the Best Cybersecurity Education Provider award in 2016. Of the three e-learning platforms evaluated, Cybrary is the only platform that focusses on cyber security.

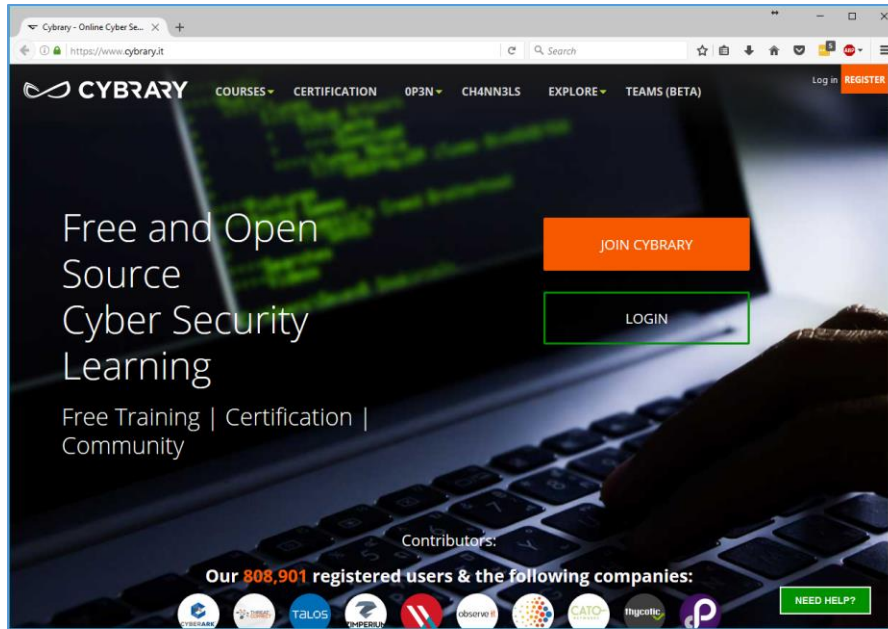


Figure 2.d: Cybrary, free cyber security training

As the e-learning environment being developed for this research is designed for use in schools, it cannot deliver content entirely by video in the same way as Cybrary. This is because students watching videos for different topics at the same time may prove distracting to other students. Some video content should be provided, however, to cater towards visual and auditory learners. These videos can be watched in students' own time, or as an entire class, with supporting text for when videos cannot be played.

In a similar fashion to the other e-learning environments evaluated, Cybrary uses gamification to encourage participation from its members. Users earn points, known as “cybytes” which add up to place users on different skill levels within the website.

Cybrary's UI design is clean and simple to use. Within each topic, a user is led onto the next video that they should watch, and upon completion of a topic, the user is suggested the next steps that they should take. As such, the user never feels “lost” within Cybrary, and can work out where to progress to next.

Cybrary was established in 2015 (Cybrary, 2016), and at the time of writing just over two years later, it has over 835,000 members (Cybrary, 2017). This rapid growth shows the scale of the need for quality cyber security e-learning resources.

2.1.4 Additional Reading

Khan (2005) outlines a number of components and features which should be implemented into e-learning environment as they are conducive to the learning experience. One of the key components is “Ease of Use”. This relates back to the UI design, as discussed with each evaluated e-learning platform. Khan (2005) explains how a good user interface can reduce students' frustration with the system and can reduce the likelihood of them losing interest. Khan

also explains that interactivity is important and that if students can interact with each other, instructors, or the resources, then they are more likely to engage with the e-learning platform. Engagement through interactivity is also discussed by Kearsley & Shneiderman in their Engagement Theory (Marshall, 2007; Khan, 2005).

Gamification has also been identified as an important aspect to encourage engagement and learning within an e-learning platform through the analysis of the three platforms. Raymer (2011) discusses the implications of gamification alongside the importance of good user interface. A number of conclusions can be drawn from the literature read regarding e-learning, and these are discussed in the following section.

2.1.5 Conclusion

A wide number of e-learning platforms exist which help to remove boundaries and restrictions to learning (Talent LMS, 2014). Through online learning platforms such as those evaluated in the previous sections, people are able to learn new skills. A number of key points have been taken about each e-learning platform in order to determine which elements should be considered when developing the e-learning environment for use in delivering the cyber security curriculum in schools.

Each of the evaluated e-learning platforms utilise gamification to engage students. Barata *et al.* (2013) have performed extensive research into gamification of an engineering course and provide a number of guidelines that developers should consider when gamifying courses. Barata *et al.*'s research shows a clear improvement in students' grades who used the gamified course over those who used the traditional course.

In each of the evaluated e-learning platforms, gamification has been effectively implemented to engage users. As such, the author concludes that in order to design an effective e-learning environment for the cyber security curriculum, elements of gamification should be integrated into the teaching material. Barata *et al.*'s guidelines should be considered when developing the gamification aspects. This should encourage active participation in the learning process.

Another aspect that each e-learning platform consistently implements is a clear, easy to use user interface. It is apparent that if users cannot easily use the website, then they may lose motivation to learn, and the e-learning environment is unlikely to have a positive effect on the learning experience. It is important to encourage learning through a fun, easy to use platform so that students do not even realise that they are learning.

2.2 User Interface Design

Analysis of the existing e-learning platforms has shown that good user interface (UI) design is essential for the developed application to be a success. A good UI should allow the educational resources to be viewed on a wide set of devices (Stočes *et al.*, 2015). Voutilainen & Salonen (2015) state that responsive user interfaces should be considered a priority when developing web applications. This is further backed up by Baturay & Birtane (2013) who argue that responsive UIs are essential for effective e-learning. They argue that responsive layouts on e-learning systems help to reduce wasted time and concentration on navigating the application.

There are some disadvantages of responsive designs, namely that screen reader systems often struggle with responsive systems (Baturay & Birtane, 2013). However, for the purposes of e-learning, the advantages appear to far outweigh the disadvantages.

Syaamantak & Rajeev (2015) offer a proposed framework for e-learning systems, listing a number of requirements which they deem essential for an effective system. Many of the elements that they require relate to the UI design. They state that standard recognisable icons should be used throughout the application to help minimise ambiguity and improve the speed with which users learn how to use the system. Syaamantak & Rajeev (2015) also recommend module progress indicators and clear navigation are implemented.

The literature suggests that a responsive design should be used and that it should be obvious to the user how to progress through the learning materials.

2.3 Investigation of Common Learning Types

As discussed by Ebert and Culyer (2013), there are four main types of learner. These are Visual, Auditory, Reading/Writing and Kinaesthetic learners, as shown in Figure 2.e. Neil Fleming formed the term 'VARK questionnaire' which is commonly used to help people determine their learning types (Fleming & Baume, 2006). Some research, such as that by Gilakjani (2012), only acknowledge Visual, Auditory and Kinaesthetic learners, as visual and Reading/Writer learners use similar techniques. The following sub-sections discuss each type of learner in detail. It should be noted that there are differing views as to the number and types of learner. Dunn & Dunn (1979), for example, go into detail on a number of different learning styles which are based around environmental, emotional, sociological and physical factors.

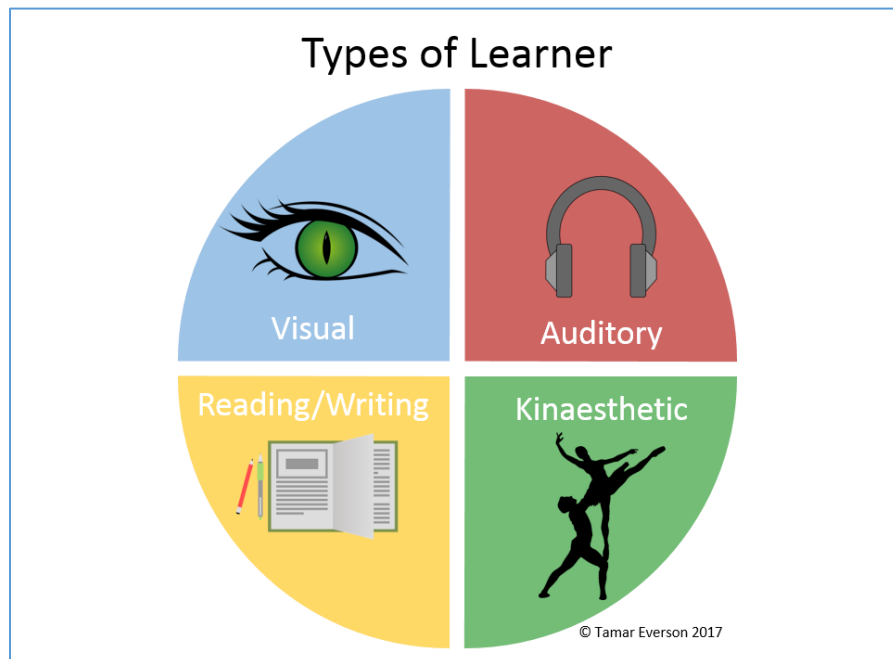


Figure 2.e: Types of learner

For the purposes of developing the cyber security e-learning environment, the four main types of learner can be used as a checklist to ensure that the content remains balanced for each learner type. The remainder of this section outlines each of these four types of learner in more detail.

Chandler & Sweller's (Sweller, 1999; 1991) cognitive load theory says that humans only have limited capacity to absorb information through different channels such as auditory or visual at a time. As such, it is important for the e-learning environment to offer a variety of channels of information to help students continue learning effectively. However, research by Kalyuga *et al.* (2004) suggests that presenting the same material in multiple forms can have a negative effect on learning. Based on Kalyuga *et al.*'s (2004) research, each way of presenting the learning material needs to have differences in the content it contains to avoid these effects.

2.3.1 Visual Learners

Visual learners look at information in a visual context in order to learn. They tend to use graphs, charts, and pictures to learn (Shattuck, 2016). According to Dunn & Dunn (1978) and Walsh (1999), 29-40% of students are suited towards visual learning.

Felder (1988) explains that visual learners “get more out of what they see than what they hear”. In order to effectively teach the cyber security curriculum to visual learners, the developed e-learning platform should utilise images, graphs and video content. Different types of textual information should also be colour coded or styled in such a way as to aid visual learners with their learning.

2.3.2 Auditory Learners

Auditory learners tend to learn through listening to content such as podcasts or by reciting information (Shattuck, 2016). Dunn & Dunn (1978) and Walsh (1999) claim that 20-34% of a typical class is suited towards an auditory style of learning.

Auditory methods which should be included in the e-learning environment to enhance the learning experience include the use of audio clips and descriptive videos.

2.3.3 Reading/Writing Learners

Reading/Writing Learners write content out and learn from written material best (Shattuck, 2016). Fleming & Baume (2006) discuss how some students prefer the written word (reading/writing learners) whereas other students prefer non-written visual information such as diagrams and graphs (visual learners). According to VARK (2015) research, 23.5% of high school students are reading/writing learners.

Most literature does not cover Reading/Writing learners, however, and merges this type of learner with visual learners. This is due to the similarities between the two learning types. As such, most statistics which refer to the number of visual learners (with the exception of VARK) are actually referring to the combined total of both visual and reading/writing learners.

The e-learning environment should encourage students to take notes as they learn in order to better cater towards their needs. By writing notes based on the materials presented within the environment, reading/writing learners are likely to better retain the information.

2.3.4 Kinaesthetic Learners

Kinaesthetic learners use practical, hands-on techniques to learn (Shattuck, 2016). By using kinaesthetic teaching methods, a teacher will engage approximately 30-40% of the class (Trinidad, 2005; Walsh, 1999; Dunn & Dunn, 1978). VARK’s (2015) research shows Kinaesthetic learning to be the most common learning type in both high school and computing students, as shown in Table 2.a below.

Kinaesthetic learning is one of the trickiest learner types to cater for in an e-learning environment. One way to make the e-learning environment suited towards kinaesthetic learners is to introduce interactive multi-choice quizzes throughout the learning material. This could then also be supported by downloadable lab work and online “try it yourself” exercises.

2.3.5 Conclusions

Whilst it is important to offer material which relates to each of the types of learner that Ebert and Culyer discuss, consideration must also be given to Chandler and his colleagues’ research. Most of the content in the e-learning environment is a combination of reading/writing and visual, including text, diagrams and charts, with a number of other media such as video, audio and multiple choice quizzes used to support the learning. By formatting the e-learning material in this way, the environment should cater towards each of the four main types of learner effectively.

Table 2.a shows the percentage of each learning type for both students in high school, and computing students, as determined by VARK (2015) research. Many of these percentages have been discussed in the previous sections. The table shows that Kinaesthetic learners are generally the most common type of learner in both high school and computing students. As such, consideration should be given to this when formulating the learning material for the students.

Table 2.a: Percentage of learner types based on VARK (2015) research

	Percentage of learner type				Total Sample size (n)
	Visual	Auditory	Reading/Writing	Kinaesthetic	
Computing Students	22.9	23.7	24.8	28.5	2,823
High School Students	22.3	25.3	23.5	28.9	10,351
Total of all participants	21.8	25.5	24.2	28.5	99,281

It is important to reiterate that some studies combine visual and reading/writing learners, making a much larger combined visual learner percentage. Different research does show discrepancies between the percentage of different learner types, sometimes in excess of 10%. The figures give a general guide which will be used to influence the design of the learning materials, but are not being considered as exact. For the purposes of this research, rough percentages for each type of learner is all that is needed.

2.4 Investigation of the Teaching Material Needed

In order to effectively educate students in line with the SQA's Cyber Security Fundamentals unit, the unit specification and other SQA literature surrounding the qualification must be investigated.

2.4.1 SQA Cyber Security Fundamentals Unit Specification

The SQA's (2015c) Cyber Security Fundamentals specification lists three primary learning outcomes for students studying the unit. Each outcome has between five and seven performance criteria. The purpose of the Cyber Security Fundamentals unit is to help people to understand and use good cyber hygiene, and it is aimed at students with no previous experience of cyber security (SQA, 2015c).

Per the SQA (2015c) specification document, the three main outcomes which a student should be able to do upon completion of the unit are to:

- 1. State common cyber security threats to individuals, businesses and nations.*
- 2. Describe routine defensive measures to minimise the risks posed by these threats.*
- 3. Secure a digital device for personal use.*

There are seven performance criteria within the specification document for outcome one. Students are required to have a basic understanding of a number of cyber security terms, and how they work. For outcome two, students must expand on this knowledge and be able to describe the terms from outcome one, as well as have an understanding of relevant legislation. Each of the SQA's outcomes are discussed in more detail in Section 4.1.2 Teaching Material Design.

The knowledge gained by students from outcomes one and two will be utilised within outcome three when the student is expected to secure a digital device and be able to identify the security features and vulnerabilities with the device.

2.4.2 Unit Assessment

The SQA have produced assessment guidance that dictates how multiple choice questions should be structured. They state that at least four options must be given for each question, one of which must be correct; the other three options must be plausible but not correct (SQA, 2015b). While the SQA provides detailed guidance on the assessment methods, it does not provide much information on the level of knowledge students should have in the curriculum. They list the

concepts that students should know but not to what level of detail. It should be noted that the SQA does not specify a set assessment method for the Cyber Security Fundamentals curriculum

2.4.3 Required Teaching Materials

A large number of teaching materials need to be developed in order to teach the Cyber Security Fundamentals curriculum effectively. For the purposes of this research, a small subset of the overall required materials has been created. A breakdown of the materials created and the learning methods used for each performance criteria has been included in Section 4.1.2 Teaching Material Design.

The Cyber Security Challenge (2017) provides a number of lesson plans for teachers on a variety of cyber security topics. Some topics relate to aspects of the Cyber Security Fundamentals Unit. The lesson plans particularly relate to the aspects of Learning Outcome 2 where students have to understand the methods used to detect and prevent attacks.

2.4.4 Conclusions

There is very little material currently online to aid teachers in their delivery of cyber security curriculums, but even over the course of this research, there has been improvements, with the Cyber Security Challenge publishing lesson plans online. Most of the teaching materials for the e-learning environment have had to be entirely created by the author.

The created materials link closely to the Cyber Security Fundamentals curriculum, with each unit within the e-learning environment directly linking back to an outcome from the unit specification.

2.5 Methods of Collection and Analysis of Data

In order to properly evaluate the effectiveness of the e-learning environment at improving the cyber security learning experience in schools, data needs to be collected and analysed. There are a number of approaches which could be taken to evaluate the effectiveness of the developed e-learning environment in enhancing the learning experience of the Scottish cyber security curriculum.

2.5.1 Qualitative Analysis

Guba & Lincoln (1989) recommend the use of qualitative evaluations that take data from multiple perspectives. As argued by Mandinach (2005), qualitative methods often give less precise measurements than quantitative methods, but provide more detailed information. Methods of qualitative data collection can include “(1) in-depth, open-ended interviews; (2) direct observations; and (3) written communications.” (Patton, 2015). The written communications can include the use of open-ended responses within questionnaires. Roffe (2002) also outlines a number of qualitative questions which can be used in the evaluation of e-learning environments.

One key advantage of qualitative research is that the researcher can get quotes and thoughts from the participants who are evaluating the e-learning environment, whereas other methods may not get the individual thoughts of participants across.

2.5.2 Quantitative Analysis

Quantitative analysis requires the collection of empirical data (Taylor, 2005). Quantitative research focusses on any data which is represented in numerical form or is measurable (Moghaddam & Moballegghi, 2008). Generally, quantitative research is conducted where there are large sample sizes that represent the entire population (Moghaddam & Moballegghi, 2008).

The number of students currently learning the cyber security curriculums across Scotland is currently around 400, with approximately one quarter of these undertaking the Cyber Security Fundamentals unit (Campos, 2017)⁶. As such, only a small sample size will be available to evaluate the developed application.

2.5.3 Heuristic Evaluation

Heuristic evaluation is commonly used to analyse the usability of applications and interfaces. It involves participants looking at the interface and giving opinions (Nielsen & Molich, 1990). Nielsen & Molich (1990) argue that heuristics is one of the most common methods of evaluating software.

Kantner & Rosenbaum (1997) argue that heuristic evaluation can identify the majority of usability problems within websites, with just two heuristic evaluators usually identifying over 50% of the problems with a website.

Heuristic evaluation is not a replacement for getting actual users to evaluate an application as they “always surprise us: they often have problems we don’t expect” (Kantner & Rosenbaum, 1997). Per Kantner and Rosenbaum’s findings, any evaluation of the e-learning environment will also use a sample of students in order to get more accurate findings than an entirely heuristic-based approach can.

The author has combined heuristic evaluation questions into the staff evaluation of the e-learning environment in order to obtain the expert views of teaching staff.

2.5.4 Conclusions

Based on the literature discussed above, the author determined that a combined qualitative and quantitative questionnaire (mixed method of research) should be issued to participants in order to obtain detailed results for analysis. The questionnaire was issued to as many different stakeholders as possible in the time available for the evaluation of the project. A questionnaire containing both open-ended qualitative and set quantitative questions was issued to members of teaching staff and students who deliver and learn the curriculum content.

⁶ The full email trail with Campos can be found in Appendix **Error! Reference source not found. Error! Reference source not found.**

Participants were asked to use the e-learning platform and fill in an evaluation based on their experiences. In order to ensure the validity of this research, careful consideration has been given to the questions that were asked about the e-learning environment, as well as the methods used to analyse the data. The formulation of the questionnaire is discussed in Section 3.1.5 Evaluation.

2.6 Conclusions

A number of factors need to be considered when developing an e-learning system to teach the secondary level cyber security curriculums. Existing e-learning platforms have already identified what works well within e-learning systems, but the author's research into learning styles has helped to identify that a mixture of resources are needed to truly make the environment accessible to all learners. Consideration of the SQA's curriculum and assessment guidelines has been given throughout the development of the system. To truly determine the effectiveness of the e-learning environment within schools, research has also been undertaken into the methods of data collection and analysis in addition to development of the resource itself. The literature discussed has provided valuable insight into all aspects of the project's lifecycle and development process.

3 Problem and Systems Analysis

This project aimed to investigate how the development of e-learning resources would improve students' understanding of cyber security topics in relation to the new SQA curriculum, as outlined in Section 1.2.1 Research Question. In order to fully investigate this, the develop and test research methodology was used. The develop and test methodology has produced a valid teaching resource that can be applied to real learning environments, and attempts to combat the shortage of educational resources in cyber security. The application has been tested in order to determine its effectiveness in fulfilling the project's primary research question and enhancing the cyber security learning experience in schools.

Oates (2006) says that develop and test projects must “contribute knowledge in some way”. The project can be either the primary research focus; a vehicle to something; or it must be an end-product with the focus of the project being on the process of development. In order to contribute knowledge, the project is centred around evaluating the impact on the learning experience of cyber security students in schools that e-learning can present. This has been achieved by analysis of the literature discussed in Section 2 Literature Review, developing an application based on the literature and existing technologies, and finally by evaluating the effectiveness of the application through the use of questionnaires.

The develop and test methodology has been used as there are not currently any other cyber security e-resources available for the Scottish Cyber Security curriculums. In order to test the effectiveness of an e-learning solution in this context, an environment first had to be developed.

The project has been completed within the Computing, Communications and Interactive Systems department of Glasgow Caledonian University along with input from the SQA and school teachers on which methods will be most successful. Representatives from Scottish schools evaluated the application as they represent the target audience of the final application. The requirements analysis, design, implementation and evaluation of the project are detailed in the following sections of this report.

3.1 Project Methods

This section outlines the major steps which have been undertaken by the author throughout the project in investigating the project's requirements, developing the application, and evaluating it. Figure 3.a below summarises each of the main steps involved in the development and testing of the project. Each step within the diagram is discussed within the following subsections.

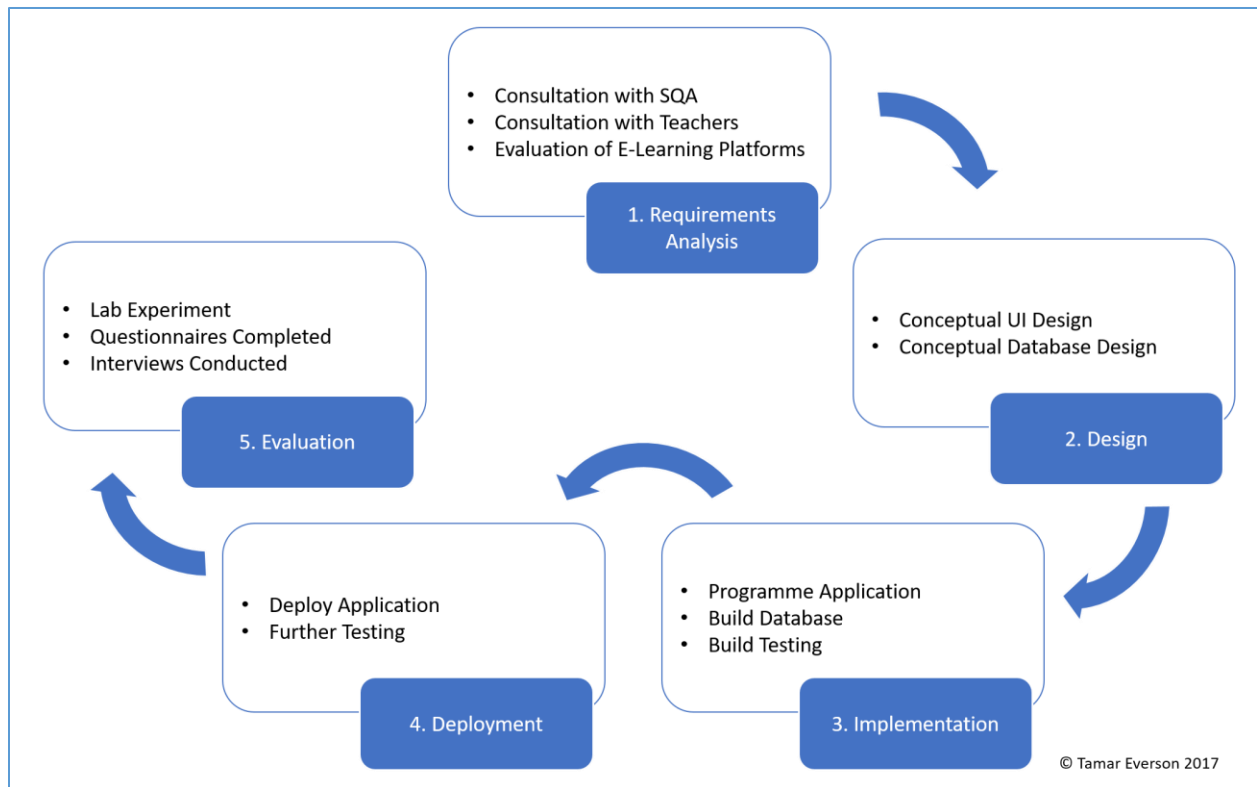


Figure 3.a: Project Development Process

3.1.1 Requirements Analysis

Requirements analysis was conducted in order to ensure that the developed application included adequate requirements to produce an effective e-learning solution. Interviews with relevant stakeholders from the SQA and teaching staff, as well as review of relevant literature was used to formulate accurate and achievable requirements. This process has helped to develop an application which is more likely to be successful in improving cyber security education in schools.

3.1.2 Design

After conversations with various stakeholders and analysis of the relevant literature, the author commenced design of the application's user interface (UI). The author initially drew up paper prototypes for the design to aid with the development process, before implementing the interface to the developed application. Full detail of the design process can be found in Section 4.1 Design.

3.1.2.1 Paper Prototypes

Paper prototypes were initially used as they save significant time over creating electronic prototypes. They can easily be modified as many times as required, in line with the project's iterative approach to development. De Sá & Carriço (2006)

Paper Prototypes have been used in multiple projects to ensure applications work and do not have major design flaws, such as Kangas & Kinnunen's (2005) development of a mobile application. Virzi *et al.* (1996) found that a similar amount of usability issues can be found from paper prototypes as from using an actual product, and the time savings over developing full-fledged prototypes is significant. Another advantage of paper prototyping is that it has a considerable cost saving over producing digital prototypes.

3.1.2.2 Final Designs

Once initial paper prototypes had been developed, further consideration was given to how to implement the designs. HTML5 became a W3C recommendation in October 2014 (O'Connor *et al.*, 2014) and was compatible with most major browsers at that time (Irish & Manian, 2013). Due to HTML5's flexibility in development, the e-learning environment is built to render HTML5 within a user's browser.

A number of other web development techniques have been incorporated in order to make both the current and future development of the e-learning system easier and future-proof. The web pages themselves are constructed using the Smarty Templating Engine in order to separate business and functional logic and ensure that the user interface is easy to adapt and change without requiring the back-end functionality to be modified heavily. This is further aided by the use of the Sass CSS Pre-processor and CSS3. With the use of these technologies, variables can be set for items such as the primary colours throughout the website and passed into elements without the entire CSS having to be rewritten.

3.1.3 Implementation

The next stage of the development process was the implementation phase. A lot of factors needed to be taken into account in order to develop a fully functioning prototype of an e-learning environment for the SQA's cyber security curriculums.

After conversations Hunter (2016), it was decided that a web-based system was an effective way of providing e-learning in schools, as schools already use other web-based e-learning environments such as Glow Connect, BBC Bitesize, and Solar (see Appendix C: Related Resources).

A number of languages and technologies have been used throughout the development of this project. These are discussed in the following subsections.

3.1.3.1 Development Language

The primary development language for the application is PHP Hypertext Pre-processor (PHP). Microsoft's ASP .NET framework was examined as it has some clear advantages over PHP in terms of in-built security functionality. However, the restrictions of running .NET applications on Windows Servers and the cost involved in licensing these servers led the author to decide to use PHP.

The author was already familiar with the PHP programming language prior to commencing the project, which is the main advantage of using PHP. This ensured that the time required to learn

the language was kept to a minimum, and the development time thus reduced. The author used an object-oriented approach to PHP development. This is because object-oriented programming works well with iterative software development (Lavin, 2006, p. xvii).

3.1.3.2 User Interface Framework: Bootstrap

Bootstrap is a framework for developing web application front ends. It is the most popular framework for responsive websites (Bootstrap, n.d.). Bootstrap is widely used in websites across the world, and as such provides a somewhat familiar user interface to anybody who has used the internet widely before. Twitter, which is commonly used by secondary school students, uses elements of Bootstrap on their website, such as the navigation menus (Otto, 2012). Bootstrap allows effective user interfaces which work across screen sizes to be developed easily and efficiently. As such, the author decided that it was a suitable framework to use to speed up front-end development due to the time constraints and technical challenges with the back-end development.

3.1.3.3 Template Engine: Smarty

Smarty is a PHP template engine which facilitates the separation of presentation and application logic (New Digital Group, 2017). Separating the two forms of logic helps to make code easier to maintain, and means that design changes can be made without affecting the application code. Whilst only the author is developing and designing the project at this stage, should the project be taken further, the use of a template engine will make the application easier to maintain for a team consisting of both developers and designers.

3.1.3.4 Style Management: Syntactically Awesome Style Sheets

Syntactically Awesome Style Sheets (Sass) is an extension to Cascade Style Sheets (CSS). It allows for the use of variables, nesting, and other techniques which make styling a website easier than that which traditional CSS can offer (Catlin *et al.*, 2015). Sass has been used to edit the styles throughout the development, but it has been converted to normal CSS before testing the web application.

3.1.3.5 MySQL

Various database systems are available for storing the application's data. However, the most common database to be found in use with PHP, particularly on Apache servers which this application is being developed on, is MySQL. MySQL is the "world's most popular open source database" (Oracle Corporation, 2017), and is used by multinational companies around the world including PayPal, Google, Facebook and Amazon (Oracle Corporation, 2017). MySQL is a Structured Query Language (SQL) relational database management system. It is a very flexible database system which suits the project's needs extremely well. Further information about the database's structure can be found in Section 4.1.1.2 Final Database Structure.

3.1.3.6 Development Integrated Development Environment & Software

JetBrains' PhpStorm was selected as the Integrated Development Environment (IDE) to develop the application. NetBeans was initially considered due to the author's experience with the IDE,

but PhpStorm's native support of PHP 7 led to it being chosen as the development environment. PhpStorm also syntax highlights and auto-completes the other languages being used within the project, including CSS, HTML, Sass, Javascript, and SQL. This has significantly increased development time over using a text editor or similar method of development.

3.1.3.7 GitHub

GitHub is a tool used for hosting code. It is one of the largest and most popular repositories of code in the world (Github, 2017). It is useful for tracking changes and issues with the code, backing up the code, and reverting changes should an update break something with the application. This is through the version control system (VCS) Git. It also works as a method of backing up the application code should the author's primary development machine fail. PhpStorm integrates directly with GitHub to allow code to be committed, pushed and pulled as needed by the author with minimal time (Balliauw, 2013), making both PhpStorm and GitHub useful tools for the project's development.

3.1.4 Deployment Testing

At every stage of the development process, as well as on the final deployment prior to evaluation, the developed application has undergone rigorous testing by the author. Test methods have been developed for each class within the programme. These methods accept various parameters for functional testing to take place of each function within the application. The ongoing testing as part of the overall development process is discussed in detail in Section 5.1.1 Development and Post-Deployment Tests.

3.1.5 Evaluation

The final stage of the research was to evaluate the e-learning environment. As discussed in Section 2.5 Methods of Collection and Analysis of Data, this involved an evaluation by teaching staff, as well as an evaluation by schoolchildren. An outline of each of the evaluation methods is given in the following subsections, along with full detail in Section 5 Testing and Evaluation.

3.1.5.1 Staff Analysis

Albion (1999) successfully used a heuristic evaluation in the development of educational multimedia. Albion (1999) states that heuristic analysis is very useful for education as it saves both time and money over other methods of evaluation and allows for one of the most effective forms of evaluation for the resources it requires. The benefits and drawbacks of using heuristic evaluations are fully discussed in Section 2.5.3 Heuristic Evaluation. The questionnaire supplied to the teaching staff alongside the e-learning prototype is available in Appendix E: Evaluation Forms. This questionnaire contained a mixture of questions including heuristic-based questions.

3.1.5.2 Schoolchildren Analysis

As discussed in Section 2.5.4 Conclusions, A questionnaire using both qualitative and quantitative questions was developed for the schoolchildren to use when evaluating the e-learning environment. It allows for elements of a heuristic analysis to be undertaken, but also allows the students to provide qualitative feedback in the form of open ended questions. The

questionnaire that was issued to the students, as well as the parental consent forms are available in Appendix E: Evaluation Forms.

3.2 Lifecycle

The development process has used an iterative approach to software development. An iterative approach helps to manage risk as the software is tested at the end of each iteration to identify bugs and potential flaws in the design and implementation of the software (Microsoft, 2016a). The iterative design process is illustrated in Figure 3.b.

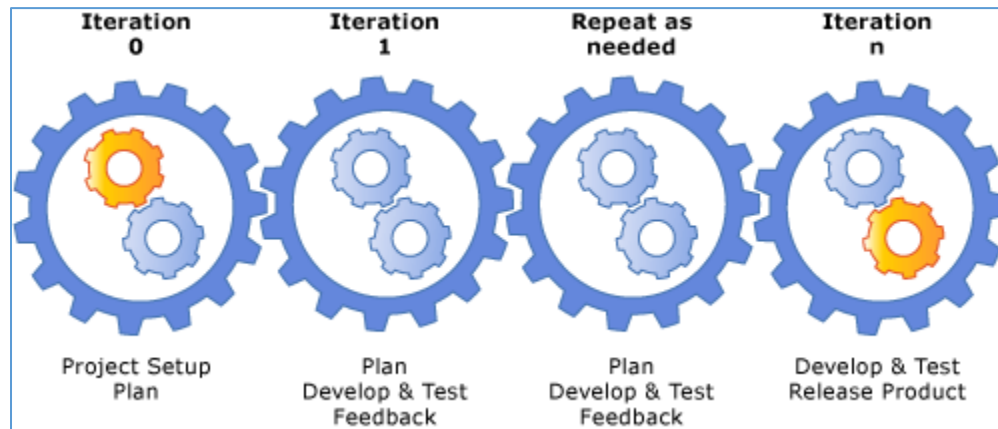


Figure 3.b: Iterative Development (Microsoft, 2016b)

The iterative approach has a number of advantages over other software development methods. One common reason for the failure of large-scale projects is that user requirements are inadequately scoped (Iqbal *et al.*, 2005). The use of an iterative approach helps to identify any oversights in the scoping process in time to take corrective action in following iterations. An iterative approach allows a working model of the software to be created at an early stage of the development process. This makes it easier to find bugs earlier in the development process, allowing corrective measures to be taken in future iterations.

3.3 Requirements Analysis

As technology has evolved, more people are using computers than ever before. Data from the Office of National Statistics shows that 82% of UK 16-24 year olds were using computers on a daily basis in 2015 (Statista, 2017b), and Eurostat shows that the UK has a 12% higher daily computer usage rate than the rest of the EU as a whole (Statista, 2017a). This data is presented in Figure 3.c and Figure 3.d.

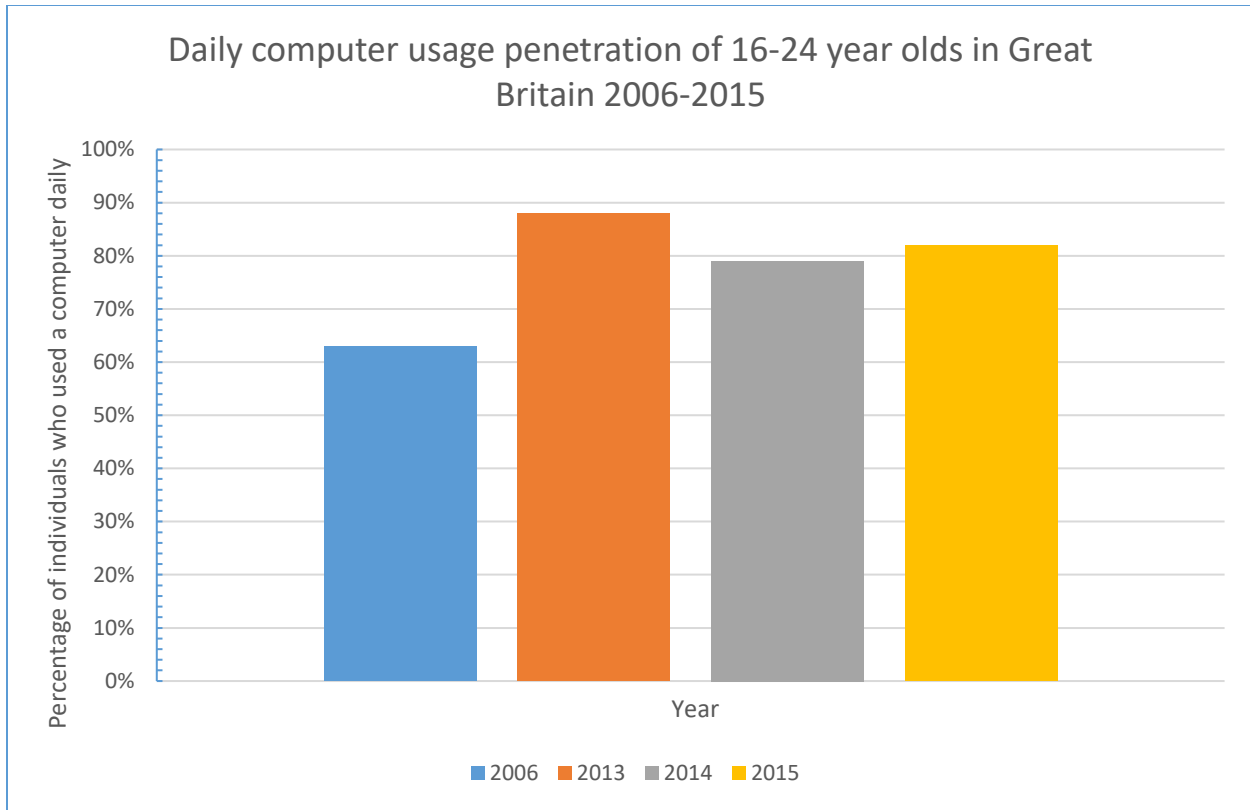


Figure 3.c: Daily computer usage penetration of 16-24 year olds in Great Britain 2006-2015 (Statista, 2017b)

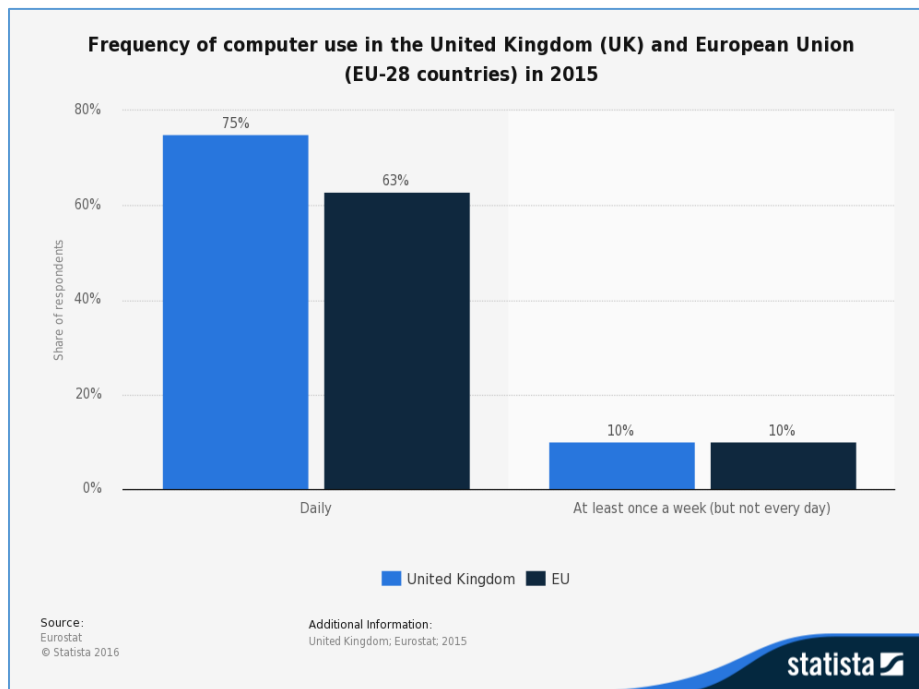


Figure 3.d: Frequency of computer use in the UK and EU in 2015 (Statista, 2017a)

This increased reliance on technology has led to a huge increase in cybercrime (Chung *et al.*, 2006). In order to educate users about cyber risks, the SQA has developed the Cyber Security Fundamentals curriculum. This application is intended to provide a learning environment to help with the delivery of the curriculum and alleviate the lack of teaching resources available for the new curriculum. The project has emerged from conversations with teaching staff and the SQA with regards to the curriculum and difficulties in effectively teaching it.

3.3.1 Interviews

Interviews were conducted in an informal setting in order to gather the opinions of the various stakeholders who participate in the development and delivery of the Scottish Cyber Security curriculums. The interviews were conducted in a conversational format with the author.

The key aims of the interviews were to:

- Identify what level of guidance teachers currently receive in delivering the cyber security curriculums
- Clarify the need for additional teaching resources for the cyber security curriculums
- Identify some functional and non-functional requirements that the teachers and SQA consider should be part of the developed solution

3.3.1.1 Initial Interview with Teacher

A telephone interview was conducted between the author and Scott Hunter of Airdrie Academy. The main aim of the interview was to establish what resources teachers already have available for the cyber security curriculums. Methods of assessing students through the platform were also discussed. A full summary of the interview is available in Appendix **Error! Reference source not found. Error! Reference source not found.**

3.3.1.2 Initial Interview with SQA

An initial meeting was held with Alastair MacGregor and Bobby Elliot of the SQA at the SQA head offices in Glasgow. The meeting's aims were to identify what learning resources the SQA felt were needed for the new Cyber Security curriculums. A full summary of the interview is available in Appendix **Error! Reference source not found. Error! Reference source not found.**

3.3.2 Literature

Existing e-learning platforms have been analysed in order to identify what works well and what does not work so well in online education delivery methods. These results are discussed in detail in Section 2 Literature Review.

3.3.3 Identified Functional Requirements

After discussions with stakeholders in the curriculum and review of relevant literature, a number of functional requirements were identified, as well as a number of recommended features.

The main functional requirements are listed below along with justification as appropriate:

FR1: Allow Students & Teachers to Authenticate

In order for teachers to view students' progress within the application (as per functional requirement 3), students' data must be securely stored and attributed to that student. Their progress should only be made available to those authorised to view it in line with the *Data Protection Act 1998*. The protection of users' data via authentication is especially important as the application will store the data of children.

FR2: Provide a range of teaching materials

The purpose of the developed system is to evaluate the effectiveness of e-learning for cyber security education. The SQA's Cyber Security Fundamentals curriculum outlines a number of areas that students must learn. These areas are discussed in the literature Section 2.4 Investigation of the Teaching Material Needed.

FR3: Allow Teachers to view Students' progress through the teaching materials

In order to be able to perform their job, teachers must be able to view their students' progress within the application. This allows them to identify students who are struggling with the curriculum, as well as those who are ready to move onto the next topic.

FR4: Allow progress quizzes for students

As per functional requirement 3, teachers need a method of monitoring students' progress. An effective way for them to do this, and for students to monitor their own progress is through the use of progress quizzes. The progress quizzes must be structured as per the SQA's (2015b) assessment guidelines in order to provide a familiar assessment process.

3.3.4 Identified Non-Functional Requirements

A number of non-functional requirements were also devised after the interviews and literature review. Analysis of literature and existing e-learning platforms highlighted the need for an easy to use user interface. It became apparent that the user interface should be familiar to users of other websites. The number of steps needed to navigate the site should be minimal and intuitive.

The following non-functional requirements were decided upon:

NFR1: There must be a clear and simple user interface

Evaluation of existing e-learning platforms has identified the implementation of a clear and simple user interface as a common trait (Section 2.1 Evaluation of Existing E-learning Platforms). Further review of literature in relation to user interface design has reinforced the need for this to be carefully considered during the development process.

NFR2: The number of steps to navigate between pages should be minimal

As with the user interface design, the navigation process within the application should be straightforward and not require an excessive number of clicks. This would reduce the number of pages that students need to load when using the application.

NFR3: The application should be easy to maintain

If the source code is not well structured and easy to modify, then future work to improve and maintain the e-learning system becomes significantly more challenging. For the purposes of this project, a prototype environment has been developed, and this should easily be expandable into a fully-fledged version for use in schools across Scotland.

NFR4: Sensitive application data should be secured

Sensitive user data such as names and email addresses should be encrypted within the database, as recommended by the Information Commissioner's Office (2012). This is because the application is storing the data of children, and as such additional safety precautions should be taken to ensure the children's online safety.

NFR5: The range of teaching materials must suit each type of learner

Review of literature identified four distinct types of learner. Each type of learner should have material which will suit their learning style within the e-learning system. This should improve the learning experience for all types of learner, and not just one or two types of learner.

3.3.5 Evaluation Participant Requirements

Two distinct groups of user were required for the evaluation phase in order to ensure that the research is fully representational and academically sound. It was decided that by getting both students and representatives from teaching staff to evaluate the e-learning environment, the research would be able to take into account both viewpoints when determining the success of the research and answering the research question posed in Section 1.2.1 Research Question. The requirements for each user type are outlined in the following subsections.

3.3.5.1 Student Participant Requirements

Secondary school students are the demographic who will be using the finished application the most, and as such the author deemed it necessary to have these students assess the e-learning environment to help assess the research question.

As such, student participants were required to be of secondary school age in order to participate. As most secondary school pupils are under the age of 16, it was necessary to obtain parental consent from the participants. All student participants were required to have parental consent regardless of age. This is firstly due to the fact that participants' ages were not asked in the research as it was not deemed necessary information, and secondly to ensure that consent was given for pupils from other countries such as England where the parental consent age is higher.

3.3.5.2 Staff Participation Requirements

Just as important as the students who will be learning through the e-learning environment are the teachers who deliver the classes. They need to be able to easily access information about their students and feel comfortable navigating the application. They also have a better idea of what the learning outcomes for the course are than the students themselves do. As such, the author felt it vital to also obtain feedback from staff such as members of the SQA or teaching staff in order to build a complete picture as to the effectiveness of the e-learning environment.

The requirements for the staff evaluation were less strict than those for the student requirements. The staff were required to have a knowledge of the cyber security curriculums and of the teaching system within Scotland. As staff can be considered experts, a large sample is not needed for the evaluation, and one or two staff members is enough to give a heuristic style of analysis.

3.4 Conclusions

This project uses the Develop and Test methodology to test the effectiveness of e-learning to deliver cyber security content. Careful consideration has been given to the problem, and project requirements drawn up for the design and implementation stage of the project. The technologies used within the project have also been discussed.

4 Design and Implementation

This section outlines the design and implementation decisions that the author has made in the development process for the project. These decisions are based on the requirements identified in section 3.3 Requirements Analysis. The design, implementation and deployment of the application will be detailed in the following subsections along with detail on how the application has been tested throughout the development process. The iterative design process will be detailed along with a description of how each phase contributed to the final application, and allowed the author to evaluate the effectiveness of the application.

4.1 Design

This section outlines the full design process for the application and discusses each of the iterations in the development process. The author evaluated the designs in relation to the literature on UI design (as discussed in Sections 2.1 Evaluation of Existing E-learning Platforms and 2.2 User Interface Design) before final UI designs were created prior to implementation.

4.1.1 Initial Application Design Concepts

Before development began on the application, initial design documentation was drawn up. This initial documentation is discussed in the following subsections.

4.1.1.1 Initial User Interface Design

Initial designs for the user interface of the application were drawn up by the author early on in the project in order to work towards functional requirement NFR1: There must be a clear and simple user interface. These attempted to provide clarity on what the final application would encompass, as well as ensuring that each of the functional and non-functional requirements was addressed in one of the proposed iterations in the development process.

Initial concepts for various key screens within the application are shown in the following subsections. Concepts for all screens are shown in Appendix G: Design & Functionality.

4.1.1.1.1 Login Screen

Functional Requirement FR1 states that users must be able to authenticate to the application. This is addressed by implementing a login screen. Figure 4.a shows the conceptual design for the login screen. There is a single login screen for all user roles. This allows users who have multiple roles (e.g. school administrator and teacher) to access all of their functions from one single login.

Hand-drawn wireframe of a login page. The page title is "Login". The URL is "/login" and the authentication level is "0". The page has a navigation bar with "Site Name", "Home", "About", "Register", and "Login" links. The main content area contains a "Login" form with "Username" and "Password" input fields, a "Login" button, and links for "Forgot Password?" and "Register". A green label "Login Form" with a pointer indicates the form area.

Figure 4.a: Login Page

4.1.1.1.2 User Dashboard Design Concept

Figure 4.b shows the conceptual design for the profile page (hereon known as “dashboard”). The dashboard is the default page that a user is shown when they log in.

Student View

As per the initial design concept, the page should show the student’s current progress, with a link to continue with the next topic to the one previously completed. A link to a list of topics which students have flagged for revision should also be prominently placed on the dashboard. Statistics should also be shown to the user in order to bring an element of gamification to the system, as discussed by Barata *et al.* (2013).

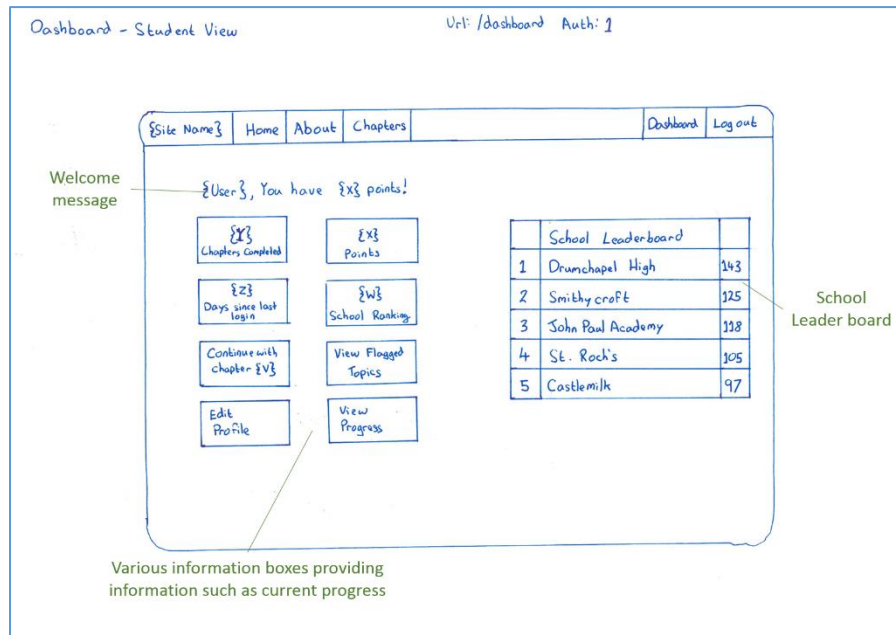


Figure 4.b: User Dashboard Design Concept

Hunter (2016) proposed an inter-school leader board which would encourage participation as students are likely to want to beat the other schools on the board. This leader board is shown in the design concept, but has not been implemented in the initial release of the application due to development time constraints. Further information on the leader board is discussed in 6.4 Future Work.

4.1.1.1.3 Chapter Overview Page

As per the initial design concept, each major topic within the e-learning environment should have an introduction page outlining the major learning objectives within the chapter. There should be a navigation bar down the left-hand side of the screen to allow users to navigate to specific topics within the chapter, as well as a button placed beneath the description to lead the user onto the first topic within the chapter. An image or introductory video will be displayed on the right-hand side of some pages. The conceptual sketch for the Chapter Introduction page is shown in figure Figure 4.c.

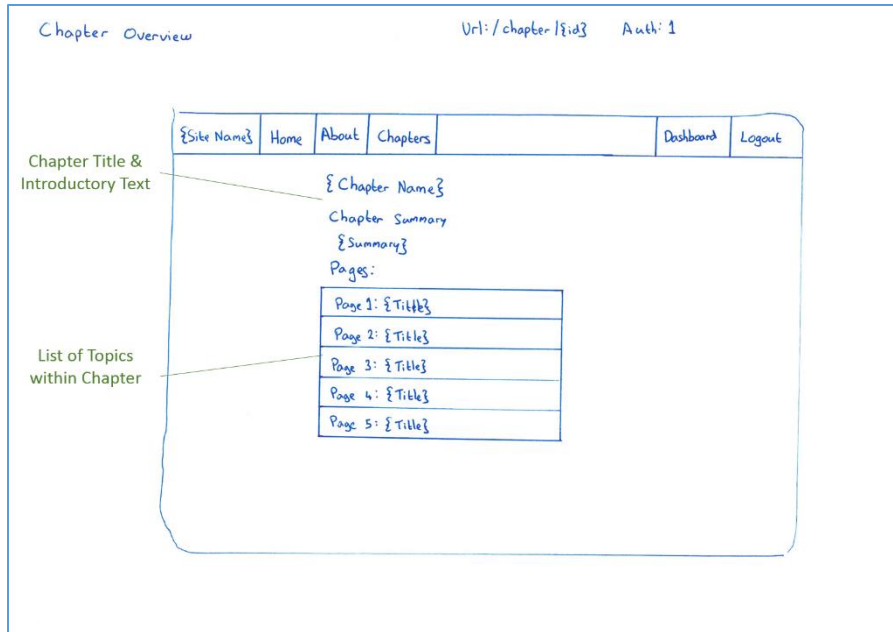


Figure 4.c: Chapter Introduction Design Concept

4.1.1.1.4 Topic Page

Each chapter should consist of a number of topics based on the SQA curriculum (discussed in Section 4.1.2 Teaching Material Design). Each topic should be displayed on its own page within the e-learning system, and consist of text for the user to read. Some topics may have videos or audio to help to explain the concepts within the topic. Each topic could also have buttons that the user can click to add the topic to a revision list or flag the question so that the teacher knows that the student needs more help with the topic. A conceptual design for the topic pages is shown in Figure 4.d. Both students and teachers have an almost identical view of the topic pages.

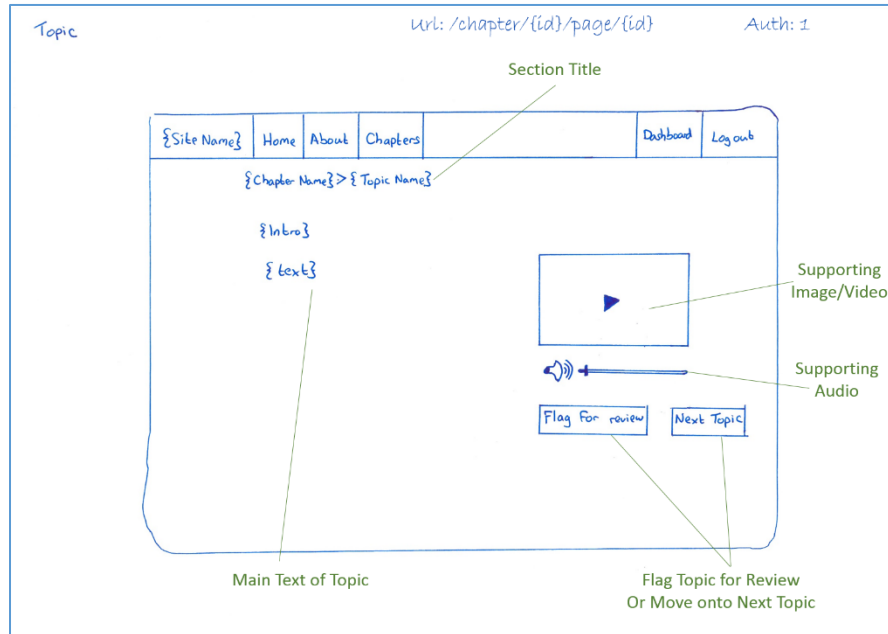


Figure 4.d: Topic Within Chapter Design Concept

4.1.1.1.5 View Classes Page

Teachers should have the ability to view each class that they teach. This shows the number of students that are in each class, as well as information about any messages or help requests sent by students to the teacher. A conceptual design for this page is shown in Figure 4.e. Students can see which classes they are attached to on the same page.

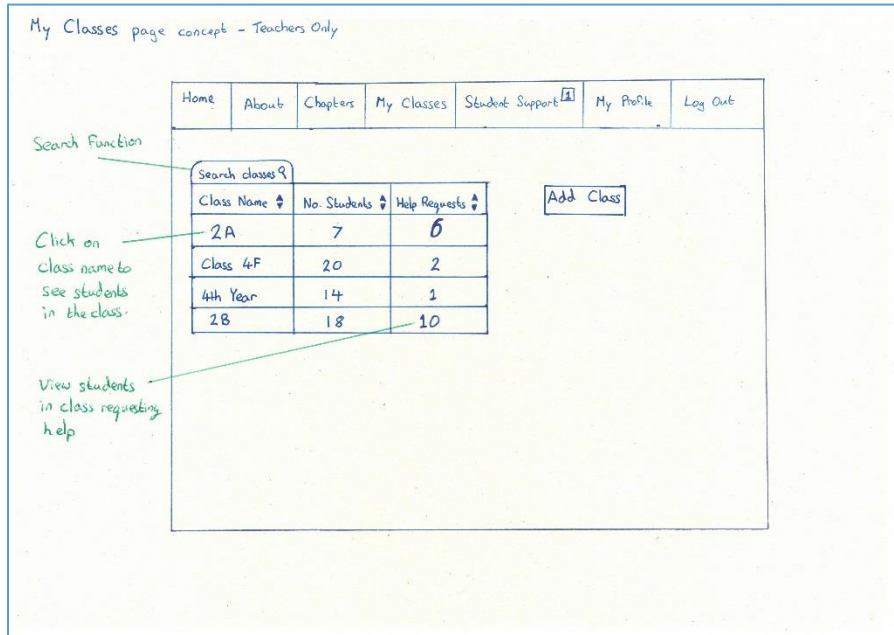


Figure 4.e: My Classes View Design Concept

4.1.1.1.6 View Students Page

Teachers are able to view information about each student in a class, including the topic that they last looked at, and any help requests or messages that they have submitted. The teacher will also be able to view detailed information about each individual student and their progress. A conceptual design for this page is shown in Figure 4.f.

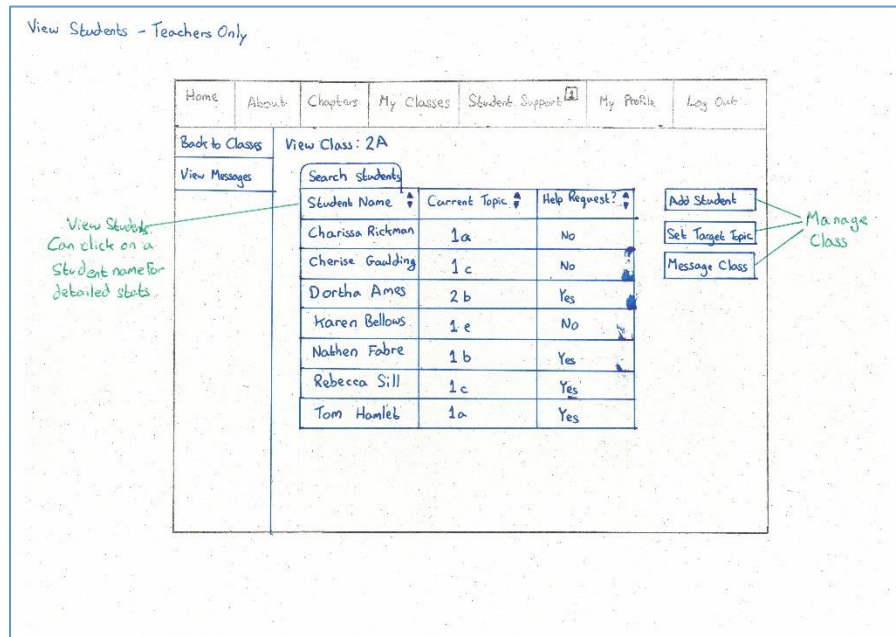


Figure 4.f: View Students View Design Concept

4.1.1.2 Final Database Structure

The final database schema can be seen below in Figure 4.g. A larger image can be found in Appendix H.2: Final Database Schema. The application's database schema uses the Crow's Foot database notation. Crow's Foot is a commonly used method of displaying database schemas in a clear manner, showing attributes including primary keys, foreign keys and relationship types (Cherwinka, 2012).

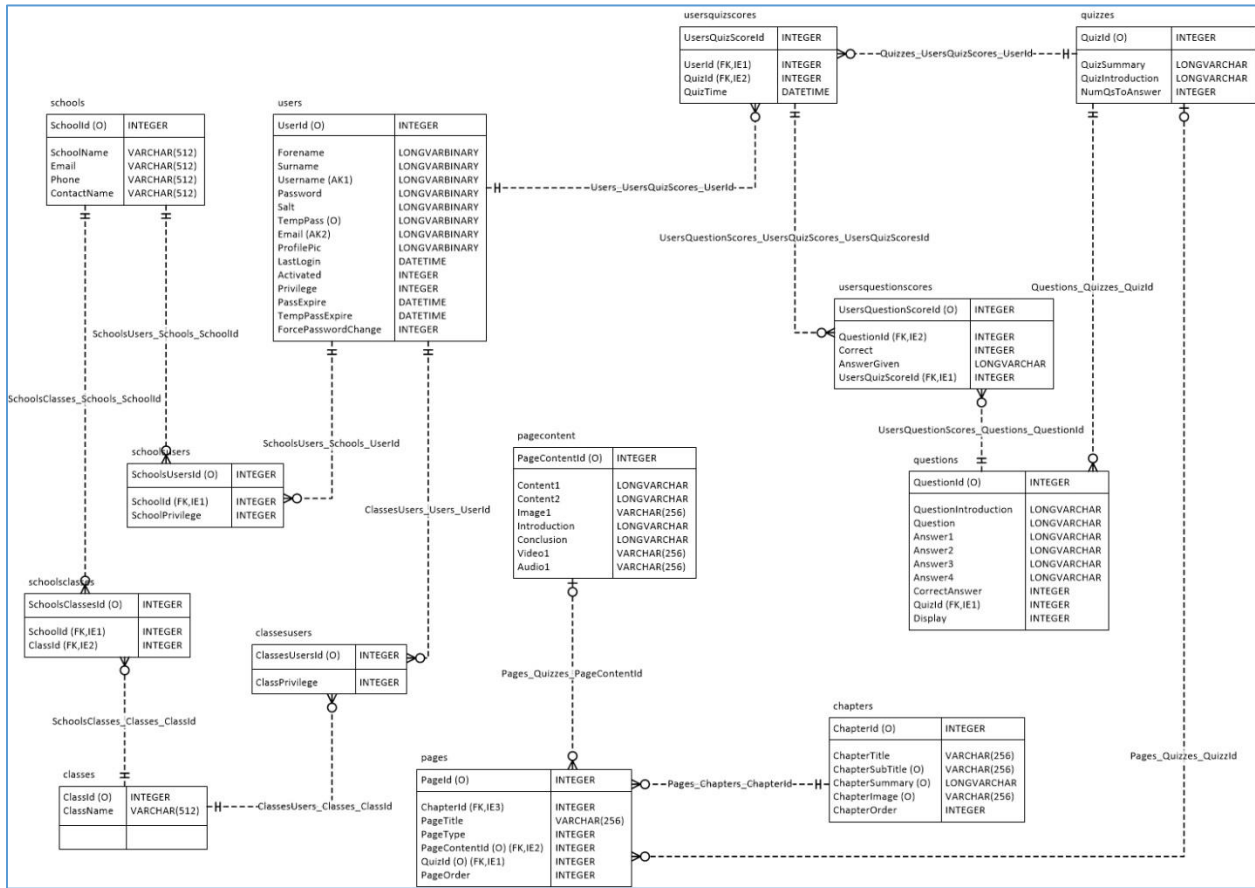


Figure 4.g: Final Database Schema

A key for the various symbols in Crow's Foot notation is shown in Table 4.a.

Table 4.a: Crow's Foot Notation Key

Notation	Meaning
	One and only one
	One or many
	Zero or one
	Either zero, one, or many

4.1.1.3 Final Navigation Structure

Per non-functional requirements *NFR1: There must be a clear and simple user interface* and *NFR2: The number of steps to navigate between pages should be minimal*, the way in which users can navigate the application is particularly important. As such, the e-learning application's navigational structure has been carefully considered by the author. The final structure for each of the three main user roles (unauthenticated, student, teacher) is shown in Figure 4.h, Figure 4.i, and Figure 4.j.

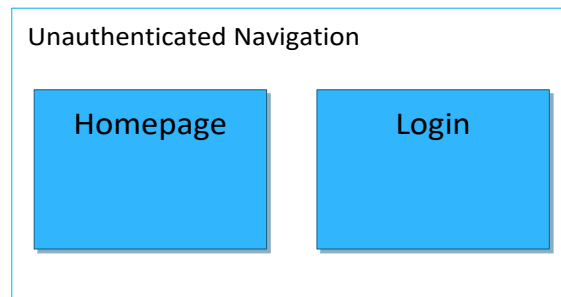


Figure 4.h: Unauthenticated User Navigation

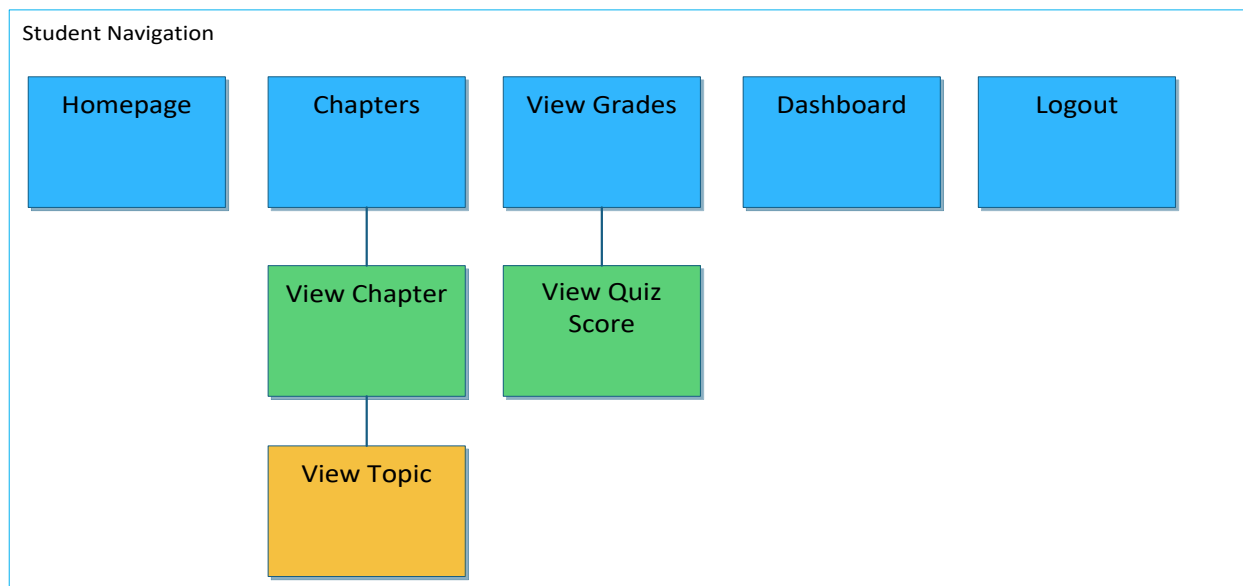


Figure 4.i: Authenticated Student Navigation

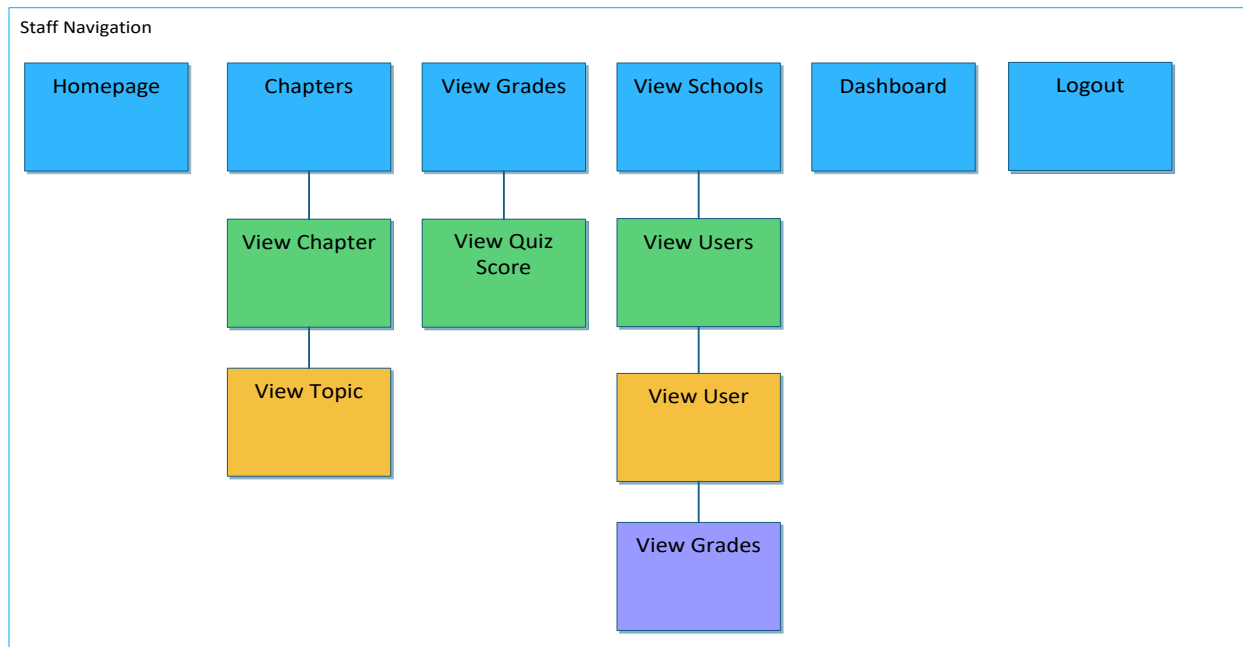


Figure 4.j: Authenticated Teacher Navigation

4.1.2 Teaching Material Design

In order to fully test the effectiveness of e-learning in delivering the SQA’s (2015c) Cyber Security Fundamentals unit, teaching materials needed to be created. Each of the SQA’s learning outcomes are discussed in the following subsection, followed by a detail of the produced materials.

4.1.2.1 SQA Learning Outcomes

The outcomes listed in the following subsections are taken directly from the SQA’s unit specification documentation. They detail the learning outcomes and performance criteria for the Cyber Security Fundamentals Unit.

4.1.2.1.1 Outcome 1

Outcome 1 has seven performance criteria, as outlined below:

- a) *State the growth of digital technologies, digital networks and digital data.*
- b) *State the scale of, and reasons for, the growth of cybercrime.*
- c) *State the potential motivations of malicious hackers.*
- d) *State common vulnerabilities in digital devices and digital networks including social engineering techniques.*
- e) *State how these vulnerabilities can be used to attack individuals, businesses and nations.*
- f) *State the potential risks to personal privacy posed by these vulnerabilities.*
- g) *Use terminology correctly in the context of cyber security threats.*

(SQA, 2015c)

4.1.2.1.2 Outcome 2

Outcome 2 has six performance criteria, as outlined below:

- a) *Describe the security measures that can be taken to reduce vulnerabilities in terms of actions, devices, procedures or techniques.*
- b) *Describe personal behaviours that minimise the risk of a successful attack.*
- c) *Describe the ways in which attacks can be detected.*
- d) *Describe the ways in which individuals and organisations can respond to attacks.*
- e) *Describe contemporary legislation relating to the protection of data, computer systems and personal privacy.*
- f) *Use terminology correctly in the context of cyber security defence.*

(SQA, 2015c)

4.1.2.1.3 Outcome 3

Outcome 3 has five performance criteria, as outlined below:

- a) *Identify the hardware and software security features in personal digital devices.*
- b) *Identify the types of vulnerabilities in personal digital devices.*
- c) *Identify defensive measures to minimise the risk of an attack on personal digital devices.*
- d) *Configure the security features in personal digital devices.*
- e) *Test the security of personal digital devices.*

(SQA, 2015c)

4.1.2.2 Design of learning materials

The literature review (Section 2.3 Investigation of Common Learning Types) identified a number of key learning types which the e-learning application must cater towards. Analysis of existing e-learning platforms (Section 2.1 Evaluation of Existing E-learning Platforms) helped the author to decide on a number of methods for delivering the learning resources.

Each topic within the application has a body of text which students are expected to read in a similar fashion to textbooks. The text contains real-world examples and case studies to help students to understand and comprehend the information.

Where the author feels that it is useful to the student, audio-visual materials have also been provided. This includes the use of videos, audio tracks, and images. Quizzes have also been produced at intervals within the teaching materials in order to test students' knowledge of various topics.

4.1.2.3 Performance Criteria Targeted

The e-learning environment which has been constructed is an alpha-version application designed to test the effectiveness of e-learning at the secondary level for cyber security (see Section 1.2.1 Research Question). As such, learning materials for all outcomes and performance criteria have

not been produced. Materials for Performance Criteria a, b and c of Outcome 2 has been produced for the purposes of this evaluation.

4.2 Implementation

The following subsections outline the development of the application based on the design choices outlined in Section 3 Problem and Systems Analysis. Details of the code produced as well as the methods used to test it throughout development are discussed.

4.2.1 Application Development

After full analysis of the problem was conducted, as detailed in Section 3 Problem and Systems Analysis, full development of the e-learning environment commenced. The design prototypes that had already been generated were used to provide a baseline structure for the system's architecture. The application consists of a *Core* class *class.core.php*, which is used within every page in the application. Additional PHP classes are used for various functions throughout the environment. The main features of the developed code are outlined in the following subsections.

4.2.1.1 Core Functionality

The *Core* class, located at */core/class.core.php*, performs a number of functions across the website. Firstly, it contains all of the variables across the website such as the website's name, URL, and database credentials, as well as information relating to the session and password security requirements. The *Core* class also contains debugging variables which allow for detailed error messages to be displayed when debugging is enabled, and controls access to restricted pages within the application. The full class can be seen in Appendix **Error! Reference source not found. Error! Reference source not found.**

4.2.1.2 Access Control

Access control is managed from the *LoginRequired* method within the *Core* class. This method runs a number of checks before allowing a user to view a page, as detailed below.

Firstly, if the user is logged into the application, it checks whether or not the user is authorised to view the requested page. If not, then the user is redirected away to a page specified by the code on the requested page (usually an error 404 page).

If the user is authorised to view the page, then the method then checks the validity of their password. If it has expired, then they are redirected to the force password change page within the application. The user is unable to view an access controlled page if their password has expired until they update it. If the user passes all of the checks, then the requested page will be displayed.

Code Snippet 1 shows the *LoginRequired* method within the *Core* class. This method controls access to restricted pages within the application as detailed in the preceding paragraphs. The full source code for the application can be found in Appendix K: Source Code⁷.

⁷ Note that source code for libraries which are available from the internet are not included in the full source code within the appendix, as this would run onto thousands of pages. Detail of these

Code Snippet 1: LoginRequired method of Core class

```
63. public static function LoginRequired($privilege,$redirectIfFalse,$die=true,$checkPassExpiry=true){
64.     if(isset($_SESSION['user'])){
65.         if ($_SESSION['user']['privilege'] & $privilege){
66.             if($checkPassExpiry && $_SESSION['user']['forcePasswordChange'] == 1){
67.                 header('Location: /password-change');
68.             }
69.             return true;
70.         }
71.     }
72.     include $redirectIfFalse."";
73.     if($die){
74.         die();
75.     }
76.     else {
77.         return false;
78.     }
79. }
```

The *LoginRequired* method meets Functional Requirement *FR1: Allow Students & Teachers to Authenticate* in conjunction with the *Login* class. The *Login* class handles the authentication process in verifying users' identity when they attempt to access the secure areas of the e-learning environment.

4.2.1.3 User Assessment

Functionality has been implemented to allow quizzes on the learning materials to be generated. The quizzes have been implemented to be as flexible as possible for teachers who get their students to take assessments through the platform. Each quiz is formed of multiple choice questions, from which a student selects one correct answer out of four possible answers. This is in conformity with the SQA's (2015b) Guide To Assessment which states that multiple choice questions should contain at least four possible answers.

In order to allow the questions to be used for assessment as well as just revision, the application allows a pool of questions to be created. Within the database, a question can be flagged to one of three states, as shown in Table 4.b.

is provided in the appendix, however, and the entire application is available on Github at www.github.com/tevers200/honours. Note that this repository is access controlled, and the author must be contacted before access will be granted.

Table 4.b: Quiz Question State

Question State	Meaning
0	Do not display question
1	Display question randomly
2	Always display question

By allowing for this flexibility when creating quizzes, it allows random quizzes to be generated for each student in the class, or for the class to all take the same assessment. It allows for some set questions to be asked of all students whilst also allowing some questions to be displayed randomly from the pool for students. This flexibility will allow teachers to assess their students in whichever method they deem most appropriate whilst still having the benefits of a pool of questions set by an expert in the field of cyber security and from instant grading of results.

Additionally, through the *view-grades* page within the e-learning environment, it is possible for both students and teachers to view students' grades in a given quiz. This allows for close monitoring of student progress and the ability for teachers to identify and further assist struggling students. The implementation of the quiz and monitoring functionality addresses functional requirements *FR3: Allow Teachers to view Students' progress through the teaching materials* and *FR4: Allow progress quizzes for students*.

4.2.1.4 System Security

Non-functional requirement *NFR4: Sensitive application data should be secured* specified that application data of a sensitive nature should be kept secure. This has been achieved through a number of mechanisms within the application's logic, as detailed in the following subsections.

4.2.1.4.1 Database Storage

All sensitive information within the database including users' names and email addresses are encrypted before being stored in the database. The data is stored using an AES Cipher-Block-Chain cipher which offers good security against personal data should the application's database be breached. Additionally, passwords are hashed and salted before storage in the database as discussed in Section 4.2.1.4.2 Passwords.

4.2.1.4.2 Passwords

Passwords are hashed over 65,000 times using a SHA512 hash, and salted, before storage in the database. This means that users' passwords should never be obtainable should the database be breached.

Additionally, a password policy has been uniquely developed for the e-learning environment that encourages the use of long, complex password. Passwords are scored depending on length and number of unique characters within the password, along with a variety of other factors. If the

password's score is greater than the requirement set in the *Core* class, then the password for the user will be accepted. This function also checks users' passwords against the top 10,000 passwords (Miessler, 2014) in order to ensure that weak passwords are not used. The use of strong passwords helps to minimise the risk of an attacker gaining access to a users' account and stealing their data.

4.2.1.4.3 Forgotten Password Process

If a user forgets their password, they can enter either their username or email address into the forgotten password form, and they will be sent a password reset link. This link will expire after three hours if not used, or immediately when used. The link contains an encrypted string made up of the users' user ID and a securely generated passphrase. When this process is followed, the users' password must be changed and they will be unable to proceed using the application until the password is reset. This helps to mitigate attacks against users' accounts via a forgotten password attack.

4.2.1.5 System Maintainability


As per non-functional requirement *NFR3: The application should be easy to maintain*, the system should be easily maintainable. The use of the Smarty Templating Engine to separate functional and presentational logic helps to make the process of updating core functionality and front end design far easier as it allows specialists of the different disciplines to focus on what they know best. The use of Smarty is discussed in more detail in Section 3.1.3.3 Template Engine: Smarty. The use of Smarty also helps to create better user interfaces due to the separation of logic, helping to meet *NFR1: There must be a clear and simple user interface*.

4.2.2 Teaching Material Development

The purpose of this project_ is to evaluate the effectiveness of e-learning to deliver the cyber security curriculum at the secondary level. As a full-fledged production-ready e-learning environment does not need to be developed to determine this, a small subset of the overall teaching materials has been developed. Section 4.1.2 Teaching Material Design details the overall curriculum and the performance criteria which have been targeted in this research. As discussed in Section 2.3 Investigation of Common Learning Types, the developed teaching materials needed to cater towards all four main types of learner. This was achieved through the integration of passages of text, videos, and audio clips alongside images into the content, as discussed in the following subsections. The created materials satisfy functional requirement *FR2: Provide a range of teaching materials* and non-functional requirement *NFR5: The range of teaching materials must suit each type of learner*.

Figure 4.k shows some sample teaching materials which explain Two-Factor Authentication through the combined use of text, audio, and video.

Tamar's Honours Home Chapters My Grades My Users



Name
Tamar Everson

Username
tevers200

Last Login
Tuesday, 28 February 2017 @ 20:12

Points
[TODO]

Badges
[TODO]

Two Factor Authentication (2FA)

There are a number of security measures which can be taken in order to reduce vulnerabilities and the likelihood of being attacked. One such measure is implementing Two Factor Authentication

Overview How 2FA Works How 2FA Can Protect You

Overview

Two factor authentication is the use of two different methods of authenticating – or logging onto – a service such as a website or computer system. The two factors can be any two of:

- Something you know
- Something you have
- Something you are

Something you know

You commonly use passwords to log onto applications such as Facebook, or even this e-learning environment. A password is something you know.

Something you have

Something you have can be a USB token, a smart card, or your smartphone. Each of these can be used to help authenticate you.

Something you are

Something you are is anything that is uniquely identifiable as you. For example, your fingerprint or an iris (eye) scan.

[Previous Page](#) [Next Page](#)




Figure 4.k: Sample of Developed Teaching Materials

4.2.2.1 Text Content

The text content is the main focus of the e-learning environment as it allows students to read at their own pace and reread sections again that they struggle to comprehend. Depending on the amount of text which is given about a particular topic, the content can be displayed in one of two ways on the page. The first method, if there is a lot of text with relevant sub headings, is to show the text in a tabbed format as shown in Figure 4.k. The second method is to have all of the text in a single section as shown in Figure 4.l.

In order to ensure that text-based content is easy to read, it is formatted using frequent headings and other methods such as bullet points. By breaking large amounts of text up in this way, it will hold the students' attention better than a single block of text (Facing History and Ourselves, 2016).

The screenshot shows a user profile page for 'User Awareness Training'. The page is titled 'User Awareness Training' and is part of a system called 'Tamar's Honours'. The user profile sidebar on the left shows the user's name as Tamar Everson, username as tevers200, and last login on Tuesday, 28 February 2017 @ 20:12. The main content area has three sections: 'User Awareness Training' with a bulleted list of points, 'No Credential Sharing' with a paragraph explaining the importance of individual accounts, and 'Choose Strong Passwords' with a paragraph explaining the importance of strong passwords. There are two images: one showing a crowd of people wearing hats, and another showing a hand holding a magnifying glass over a video player with the text 'Cyber Security - Top 10 Threats' and 'Can you afford to pay the price?'.

Figure 4.1: Sample of Developed Teaching Materials

4.2.2.2 Image Content

Images are used to highlight relevant sections of text throughout the content. For example, the image on the User Awareness Training page (ID 9) in Chapter 1 (see Figure 4.1) highlights how white, grey and black hat hackers all live, breathe and work together, and how users need to remain vigilant.

4.2.2.3 Video Content

The e-learning environment has been developed to allow for either YouTube videos or mp4 format videos hosted on the website itself to be displayed to users. This allows for the flexibility of using existing videos created by other content providers, as well as for custom videos to be created for specific content. Due to time constraints when undertaking this project, no custom videos have been created for the e-learning environment as suitable videos from YouTube have been found. Figure 4.1 shows a video embedded into a learning content page. The source code which inserts videos is shown in Code Snippet 2.

Code Snippet 2: Video Display Code in /theme/default/templates/pages/chapter-page.tpl

```

50. {if $content.Video1|strstr:"youtube"}
51.     <iframe width="420" height="240" src="{ $content.Video1}" frameborder="0
    " allowfullscreen></iframe>
52.     {else}
53.     <video width="420" height="240" controls>
54.         <source src="/resources/video/{ $content.Video1}" type="video/mp4">
55.         Your browser does not support the video tag.
56.     </video>
57.     <br>
58.     {/if}

```

4.2.2.4 Audio Content

The application allows for audio clips to be uploaded to suit auditory learners. An embedded audio clip can be seen in Figure 4.1. The source code for embedding audio clips is shown in Code Snippet 3.

Code Snippet 3: Audio Embed Code in /theme/default/templates/pages/chapter-page.tpl

```
61.     {if $content.Audio1 != "" OR $content.Audio1 != NULL}
62.         <audio controls volume="0.5">
63.             <source src="/resources/audio/{$content.Audio1}" type="audio/mpeg">
64.                 Your browser does not support the audio element.
65.             </audio>
66.     {/if}
```

4.2.3 Final Application Design

The front-end design of the website uses a mainly vanilla bootstrap configuration, as discussed in Section 3.1.3.2 User Interface Framework: Bootstrap. This is mainly because of its ease of implementation and built-in responsiveness for mobile devices. The use of Bootstrap has solved non-functional requirement *NFR1: There must be a clear and simple user interface*. Screenshots from some of the key pages throughout the application are discussed below.

Learning materials are presented in a standard format across the application, with text presented on the left-hand side of the screen, and any multimedia resources on the right. This is illustrated in Figure 4.m. The navigation is consistent throughout the application to provide a user-friendly interface.

The screenshot displays a user interface for a learning management system. At the top, a navigation bar includes 'Tamar's Honours', 'Home', 'Chapters', 'My Grades', 'My Users', 'My Dashboard', and 'Logout'. The main content area is divided into a left sidebar and a central content area. The sidebar shows a user profile for 'Tamar Everson' with fields for Name, Username (tevers200), Last Login (Tuesday, 28 February 2017 @ 20:12), Points ([TODO]), and Badges ([TODO]). The central content area is titled 'Two Factor Authentication (2FA)' and includes an overview, tabs for 'How 2FA Works' and 'How 2FA Can Protect You', and sections for 'Something you know', 'Something you have', and 'Something you are'. A video player on the right shows a video titled 'What is Two-Factor Authentication? (2FA)' with a progress bar at 0:46.

Figure 4.m: Learning Material Page

Question scores are presented in separate boxes on quiz results pages in order to clearly show which questions users got correct and incorrect, with a final box along the bottom showing the quiz's overall score. This is illustrated in Figure 4.n.

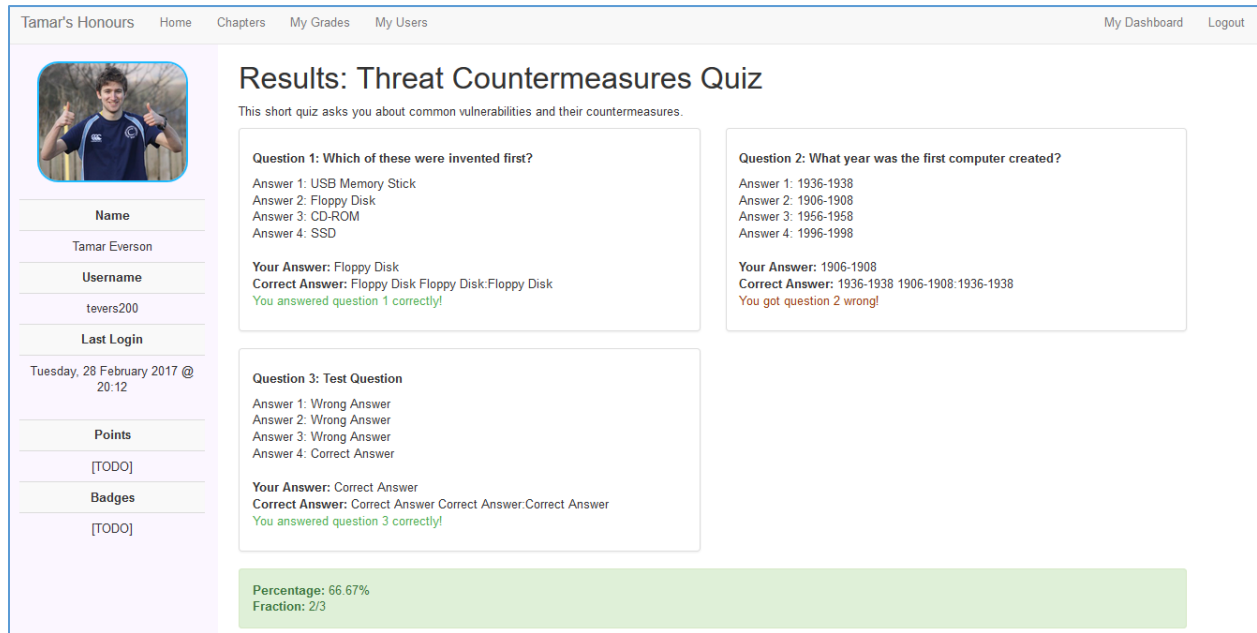


Figure 4.n: View Grades Page

4.2.4 Application Testing

A number of features and functions have been built into the application during development to allow for detailed functional testing of the application. Some of these features also work as error handling methods for the application in its day to day operation.

4.2.4.1 Try Catch Blocks

Try catch blocks were used throughout the application to catch any errors and ensure that the application terminates gracefully should an error occur. If an exception is thrown, then the `throwPHPError` method of the `ErrorHandling` class is called, as discussed in Section 4.2.4.2 Debugging Settings. A try catch block from the `User` class is displayed in Code Snippet 4.

Code Snippet 4: try catch block from User class

```

49. try {
50.     $dbconn = new Database();
51.     $stmt = $dbconn->db->prepare($query);
52.     $stmt->execute($queryParams);
53.     $row = $stmt->fetch();
54. }
55. catch (Exception $ex){
56.     $error = new ErrorHandling($ex,__CLASS__);
57.     $error->throwPHPError();
58. }

```

4.2.4.2 Debugging Settings

Debugging variables are configured within the Core class. There are three variables which configure the way in which the application is debugged, which are discussed in the following subsections. Code Snippet 5 illustrates these debugging settings.

Code Snippet 5: Debugging Settings within Core class

```
49. /** Debugging */
50. static public $debugging_mode = 10; // 0: off; 1: Minimal; 5: Verbose; 10: Verbose | recommended: 5
51. static public $debugging_method = 9; // 0: off; 1: log file; 4: html comments; 8: html page | recommended: 1
52. static public $log_path = __DIR__."/logs/.error_log";
```

When an error is thrown within the application, it calls the *throwPHPError* method within the *ErrorHandling* class, as shown in Code Snippet 6. The way the error is handled depends on the debugging settings within the *Core* class, as discussed in the following subsections.

Code Snippet 6: *throwPHPError* method of *ErrorHandling* class

```
30. public function throwPHPError($additionalMessage = "", $custom = false)
31. {
32.     $this->message = $additionalMessage;
33.     $this->custom = $custom;
34.     $log = "";
35.     $time = date("Y-m-d H:i:s")."\r\n";
36.     switch (Core::$debugging_mode) {
37.         case 10:
38.             $log .= $this->verbosityVeryVerbose();
39.             break;
40.         case 5:
41.             $log .= $this->verbosityVerbose();
42.             break;
43.         case 1:
44.             $log .= $this->verbosityMinimal();
45.         default:
46.             // do nothing
47.     }
48.     if (Core::$debugging_method & 8) {
49.         echo $log;
50.     }
51.     if (Core::$debugging_method & 4) {
52.         echo "<!--";
53.         echo $time."\r\n";
54.         echo $log;
55.         echo "-->";
56.     }
57.     if (Core::$debugging_method & 1) {
58.         $log .= "\r\n\r\n";
59.         file_put_contents(Core::$log_path, $time.$log, FILE_APPEND);
60.     }
61.     die();
62. }
```

4.2.4.2.1 \$debugging_mode

This variable sets the level of error messages which are generated. It can be set to one of four values as shown in Table 4.c.

Table 4.c: Settings for Debugging Mode

Number	Error Verbosity
0	Errors disabled. Suitable for production.
1	Minimal Error Messages. Suitable for production.
5	Verbose Error Messages. Suitable for beta and preview environments.
10	Very Verbose Error Messages. Suitable for the developer.

Minimal error messages will display the message “An Error Occurred. Terminating”. Verbose error messages will provide the name of the class in which the error occurred. Very verbose error messages contain a full stack trace for the error message.

4.2.4.2.2 \$debugging_method

This variable sets the method of logging errors using a bitwise operator. The use of bitwise operators to set the debugging method allows errors to be displayed in a combination of ways. The settings are displayed in Table 4.d.

Table 4.d: Bitwise Settings for Debugging Methods

Bitwise Number	Setting
0	Debugging is off
1	Log errors to a log file
4	Log errors to HTML comments
5 (1+4)	Log errors to a log file AND to HTML comments
8	Log errors to the HTML page
9 (1+8)	Log errors to a log file AND to HTML page
12 (4+8)	Log errors to HTML comments AND to HTML page
13 (1+4+8)	Log errors to a log file AND to HTML comments AND to HTML page

4.2.4.2.3 \$log_path

This variable configures the log file location and name. By default, errors are logged to `/logs/.error_log`, but this can be modified by changing this variable. Errors are only logged to this file if the `$debugging_method` variable is set to 1, 5, 9, or 13.

4.2.4.3 Test Pages

Test pages were implemented, as it was essential to identify and rectify as many bugs as possible before evaluation. Since it is an alpha version being developed, the evaluators could not expect the application to be entirely bug free, but any bugs within the e-learning environment would negatively impact the user experience. The use of these test pages were vital in identifying bugs during the development process.

A separate test page was generated for each class. These test pages have direct calls to each public function within the class that it tests. Data to test with can be supplied via get parameters, and the available parameters are displayed in a table at the top of the page. All test pages are available within the `/test` directory of the application, and would not be available to access in a production environment. Source code for each of the implemented test pages is available in Appendix **Error! Reference source not found. Error! Reference source not found.**. The test page for `class.passwords.php` is shown in Figure 4.o.

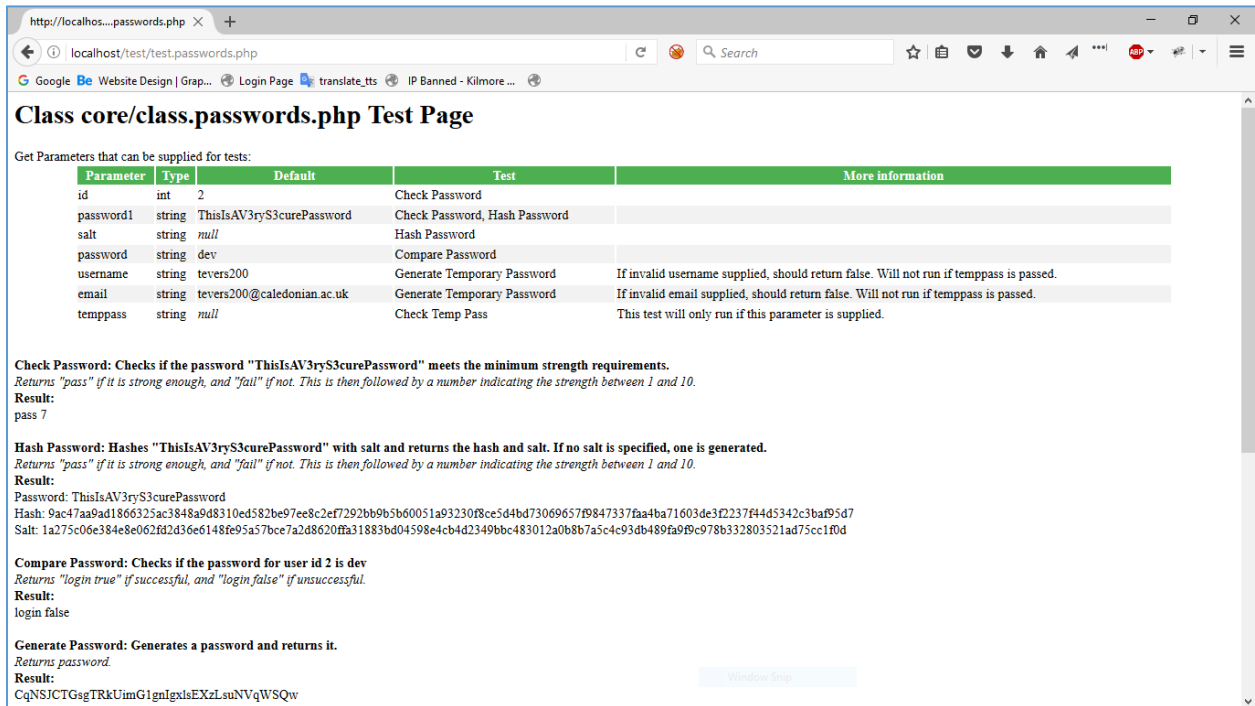


Figure 4.o: Sample Test Page

4.2.4.4 Test Data

Test data was generated for the e-learning application in order to fully test the application with different user roles and stages of progress within the environment. This data was generated from generatedata.com (Keen, 2016).

One hundred user accounts were created with varying states of activation, password expiry, and progress through the application, as well as being assigned to random classes in random schools. This has allowed the author to try out different functionality within the application without planning what outcomes should occur, better mimicking real life use cases. This test data can be found in Appendix J: Test Data.

4.3 Deployment

After the development and testing process was complete, the e-learning environment was deployed onto an Apache server online which the author already had access to. This was to allow the application to be tested in a more realistic environment than the local development server running on the author's development machine. The server and hosting specifications are outlined in Table 4.e.

Table 4.e: Server & Hosting Configuration

Processor (six cores)	Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.20GHz
RAM	8GB
Linux Version	2.6.32-042stab120.6 i686
CentOS Version	CentOS release 6.9 (Final)
Apache Version	Apache/2.4.25 (cPanel)
IP Address	212.18.228.119
Domain Name	http://ethicalhacking.org.uk

The hosting environment was chosen as the author already owns the server making it an ideal resource to host the website due to cost savings. Likewise, the author owns the domain name <http://ethicalhacking.org.uk> which suits the subject area of the e-learning environment.

In order to deploy the website, the SQL databases were extracted from the development environment and imported into a database on the web server. The code in `/core/class.core.php` was then modified to point to the production database and to generate session tokens for the correct domain, before the source code was uploaded to the server via SSH. The website then had some basic checks (as discussed in Section 5 Testing and Evaluation) in order to ensure that the production site matched the behaviours expected in the development environment. Once

these checks were complete, access to the website was given to the evaluators. The testing and evaluation process is discussed in the following chapter.

5 Testing and Evaluation

This section outlines the methods which were used in order to test and evaluate the application in order to prove or refute the hypotheses posed in Section 1.2.3 Hypotheses. The findings of the evaluation processes will be discussed and critically analysed against the aims and objectives of the project. The evaluation involved both students and representatives from the SQA performing a series of tasks within the e-learning environment, and then filling in surveys based on this usage. Each of the following subsections discuss the evaluation from the perspective of a different user group, before concluding the results ready for discussion in Section 6 Discussions and Conclusions.

5.1 Testing

A number of methods were used to test the developed e-learning environment prior to the evaluations being undertaken. This was to ensure that any bugs or major issues with the application were identified and resolved which would prevent users from effectively evaluating the application. The various testing methods which were used are discussed in the following subsections.

5.1.1 Development and Post-Deployment Tests

5.1.2 As discussed in Section 4.2.3 Final Application Design

The front-end design of the website uses a mainly vanilla bootstrap configuration, as discussed in Section 3.1.3.2 User Interface Framework: Bootstrap. This is mainly because of its ease of implementation and built-in responsiveness for mobile devices. The use of Bootstrap has solved non-functional requirement *NFRI: There must be a clear and simple user interface*. Screenshots from some of the key pages throughout the application are discussed below.

Learning materials are presented in a standard format across the application, with text presented on the left-hand side of the screen, and any multimedia resources on the right. This is illustrated in Figure 4.m. The navigation is consistent throughout the application to provide a user-friendly interface.

The screenshot shows a user interface for a learning material page. On the left is a user profile for Tamar Everson, including a name, username (tevers200), last login time (Tuesday, 28 February 2017 @ 20:12), and points (TODO). The main content area is titled 'Two Factor Authentication (2FA)' and contains a video player and an overview section. The overview section explains that 2FA is the use of two different methods of authenticating or logging onto a service. It lists three types of factors: something you know (passwords), something you have (USB tokens, smart cards, smartphones), and something you are.

Figure 4.m: Learning Material Page

Question scores are presented in separate boxes on quiz results pages in order to clearly show which questions users got correct and incorrect, with a final box along the bottom showing the quiz's overall score. This is illustrated in Figure 4.n.

The screenshot shows a quiz results page for 'Threat Countermeasures Quiz'. It displays three questions with their answers and the user's performance. The overall score is 66.67% (2/3).

Question	Question Text	Answers	User Answer	Correct Answer	Result
1	Which of these were invented first?	1: USB Memory Stick 2: Floppy Disk 3: CD-ROM 4: SSD	Floppy Disk	Floppy Disk Floppy Disk Floppy Disk	Correct
2	What year was the first computer created?	1: 1936-1938 2: 1906-1908 3: 1956-1958 4: 1996-1998	1906-1908	1936-1938 1906-1908 1936-1938	Wrong
3	Test Question	1: Wrong Answer 2: Wrong Answer 3: Wrong Answer 4: Correct Answer	Correct Answer	Correct Answer Correct Answer Correct Answer	Correct

Overall Score: Percentage: 66.67%
Fraction: 2/3

Figure 4.n: View Grades Page

Application Testing, a number of features were built into the application throughout the development process in order to allow the e-learning environment to be evaluated and tested by the author on an ongoing basis. This testing mainly comprised of tests to ensure that each section of code performed the actions that were expected.

The most useful components of the in-built evaluation functions were:

- The Debugging Settings
- The Test Pages

Each of these two functions, and how they were used to effectively test the application, are discussed in the following subsections.

5.1.2.1 *Debugging Settings*

The configuration of the debugging settings is shown in Section 4.2.4.2 Debugging Settings. By setting the debugging to very verbose and to output into the HTML page whilst testing out new functionality within the application, the author was able to quickly identify when problems occurred, and isolate the issue to a particular line of code within the application. This significantly reduced the overall development time as the author had to spend less time hunting for the source of issues when they arose.

5.1.2.2 *Test Pages*

The test pages allowed the author to utilise various functionality within the application directly without following the main application workflow. This means that the author was able to feed invalid data into various functions to see how they behaved, and if they handled errors as expected. A simple example using the *VerifyInt* method of the *Sanitise* class is discussed below.

The *VerifyInt* method takes in a value. If the value is an integer, or can be parsed as an integer, it will return *true*. If the value cannot be parsed as an integer, then it will return *false*. Within the application, every use case expects the value to be an integer. By supplying a mixture of test strings to the test page, the author was able to verify that the method behaves as expected, and to see how it responds to unexpected data. Similar testing was undertaken with every class and method throughout the application by the use of these test pages. The implementation of the test pages is discussed in Section 4.2.4.3 Test Pages.

5.1.3 *Test Cases*

A number of tests were also carried out independently from the tests built into the test pages. These were designed to ensure that the different aspects of the application were working as designed. A full list of each test conducted, including the expected and actual outcome is available in Appendix I: Test Cases.

The tests were conducted prior to the student and staff evaluations from taking place in order to check that all functional and non-functional requirements were met. By performing comprehensive tests prior to the evaluations, the author was able to ensure that there were no bugs with the application which would materially detriment the user experience within the human evaluations which were being undertaken later.

5.2 Evaluation

In order to best answer the research question posed in Section 1.2.1 Research Question, it was decided to get both students and staff to analyse the e-learning environment. This allowed the author to evaluate the e-learning system from both perspectives in order to determine the effectiveness of the application for both teachers and students. The following subsections outline the evaluations which took place and the results of these evaluations. The results are then analysed and discussed in Section 6.2 Final Discussion of Results.

5.2.1 Student Evaluation

Current students at the Secondary level were asked to perform a series of steps using the developed e-learning platform before evaluating it through a survey. The survey was designed to establish the how useful the students thought the e-learning platform itself would be in delivering e-learning content, as well as establishing the usefulness of the educational material itself in improving students' knowledge of cyber security.

Both the instructions and the survey were provided electronically, allowing students to complete the evaluation in their own time and at their own pace. As per the ethical approval process stipulated by Glasgow Caledonian University, the students' parents or guardians were required to fill out a parental consent form prior to students participating in the research. This form, along with the guidance that was provided to the students is available in Appendix E: Evaluation Forms. University of Cambridge (2015) have issued a detailed document surrounding the creation of consent forms and participant information sheets, which was used to develop the forms and information sheets for the participants in this research.

5.2.1.1 Methods

A number of eligible students were identified as per the requirements in Section 3.3.5.1 Student Participant Requirements. Each student was required to obtain parental consent to take part in the study prior to the evaluation commencing. Students were able to take the evaluation remotely from home and were issued with an information pack containing all of the required information to undertake the evaluation. This pack is available in Appendix E: Evaluation Forms. It contained a document with a series of tasks which the student was required to undertake before completing a survey which was also provided on the document.

Each student was issued with a randomly generated six-digit participant ID. This ID was used to identify the participant if they chose to withdraw from the research prior to publication. Each participant was also issued with a username and password to access the application. This was randomly assigned from the pool of test accounts which had been generated during the development testing process. It was decided to assign a random test account to each user to help maintain the anonymity of each participant.

The participant was asked to perform a number of actions within the application, including logging on, working through a unit of learning resources, and completing one of the learning environment's quizzes. Upon completion of these steps, they were then asked to complete the electronic questionnaire to provide feedback on their experience of using the application.

The questionnaire was constructed using the free popular online survey tool, Survey Monkey (2017). This allowed the full evaluation process to take place remotely, reducing the time needed to source and work with participants, as they could complete the evaluation in their own time. Users were not asked for personally identifiable information in the survey, only for their participant ID number. This ID number was matched against their names in a spreadsheet stored securely on the author's computer to track both that parental consent had been obtained and for use in the event that a participant decided to withdraw from the study. There were a mix of quantitative and qualitative questions within the questionnaire, as discussed in Section 2.5 Methods of Collection and Analysis of Data. This allowed for data to be collected that could easily be analysed statistically, as well as allowing for open-ended information to be obtained from users to more accurately get their opinion on the e-learning system.

The closed questions used a modified version of the Likert scale which incorporated a "n/a" option as well as the traditional scale of "Strongly Agree" to "Strongly Disagree". The Likert scale is a very popular scale and is frequently used in studies (Allen & Seaman, 2007; Vigderhous, 1977). By adding a "n/a" option, it allowed participants who felt that they were unable to answer a question accurately to avoid answering it and prevent skewing the data.

The questions focussed around two main aspects of the application – its usability, and the quality of the learning resources. Analysis from the literature review (Section 2) and requirements analysis (Section 3.3) identified these two areas as important to the success of an e-learning environment. The full questionnaire can be seen in Appendix E: Evaluation Forms.

As well as analysing the results from the questionnaire, the author was also able to view participants' results in the learning material quiz which was taken in the survey. By viewing the results, the author was able to gain insight into how effective the learning materials were at teaching the participants.

5.2.1.2 Results

The results were collected over two weeks towards the end of the project. In total, there were fifteen responses to the questionnaire. As discussed in Section 2.5.2 Quantitative Analysis, this is a relatively small sample for a meaningful result to be concluded. This sample, however, does represent approximately 15% of the students currently undertaking the Cyber Security Fundamentals Unit. All results to the questionnaire can be seen in Appendix F: Results. The questions asked to students were focussed around hypothesis two (See Section 1.2.3 Hypotheses) in determining the likelihood of the developed resource improving the learning experience within the cyber security curriculum.

Question one of the survey asked participants for their participant ID number for administration. Question two asked for any issues that the users faced to be outlined in order to identify usability issues and problems that would nullify users' responses. Question three asked users about the usability of the application whereas questions four to six related to the learning materials within the application and the learning process. Questions seven to ten were open ended questions allowing users to give detail on extra features or suggestions they had along with general feedback. The results are discussed in detail in the following subsections.

5.2.1.2.1 Application Ease of Use

Question three focussed on the ease of use of the application. 86.67% of respondents found the application easy to log into, with two respondents stating that they found it difficult. One user had been issued the wrong password by the author and was unable to use the password reset function. It is not known what issues the second user had. 93.34% of participants agreed or strongly agreed that the application was easy to navigate. The responses are shown in Figure 5.a.

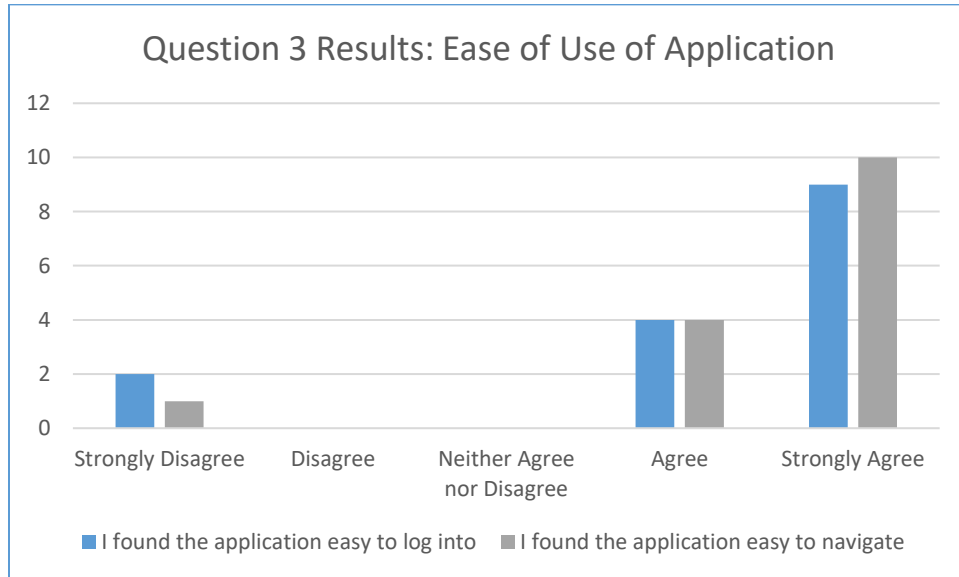


Figure 5.a: Bar Chart – Ease of Use of Application

Some participants left comments within the open-ended questions stating that the application was “very easy to use” and that they liked various elements of the user interface. Other comments suggested that the user interface could be further refined by introducing more colour and other user interface enhancements.

5.2.1.2.2 Learning Resources

Question four focussed on the learning resources and the different learning styles. Figure 5.b shows users’ preferences for the various types of learning material presented within the application. It is interesting to note that video and image resources were the two most popular resources. Text based resources were the least popular resource offered in the application, however one user noted that the formatting of the text into smaller chunks made it easier to read. 93.33% of participants found the learning resources useful with only one user disagreeing.

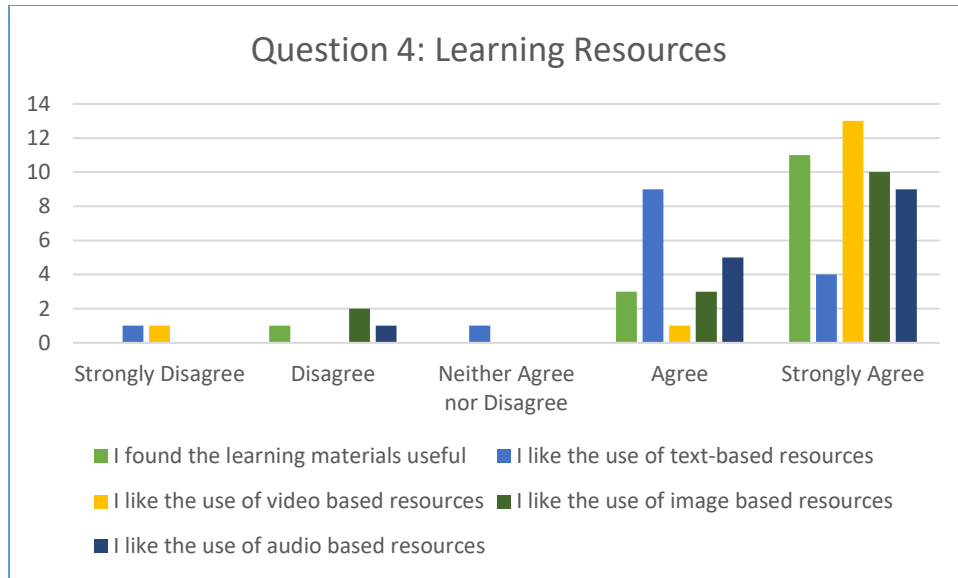


Figure 5.b: Bar Chart – Learning Resource Preference

5.2.1.2.3 Participant Comments

There are two suggestions for the e-learning environment that strongly came across in the participants' comments. The first one was the addition of games to the e-learning environment, with three of the nine respondents to question seven directly mentioning the introduction of games, with a further four participants recommending challenges or activities that are in addition to the quizzes.

5.2.1.2.4 Quiz Results

The data above indicates that students generally were strongly in favour of the methods used within the e-learning environment, and found it to be beneficial in teaching them cyber security concepts. The author has analysed the quiz results for each participant in order to determine how effective the resources may be, and see if the responses correlate to students' satisfaction with the teaching methods.

Students were asked four quiz questions during the prototype evaluation, as detailed in Appendix F: Results. No student scored less than 75% in the quiz, indicating that every participant gained some knowledge from the e-learning resources. Eleven participants scored 100%, with question three being answered incorrectly most often. The number of correct and incorrect results for each question is outlined in Table 5.a.

Table 5.a: Participant Scores

	Correct	Incorrect	Percentage Correct
Question 1	14	1	93%
Question 2	15	0	100%

Question 3	12	3	80%
Question 4	15	0	100%

5.2.1.3 Conclusions

It should be noted that the sample size is relatively small and is not large enough to accurately represent the entire population with certainty. This is further discussed in Section 6.3 Project Limitations. However, the results presented here may be indicative of the wider population, and can certainly provide some insight into the e-learning environment's effectiveness and where future work can be undertaken.

5.2.2 Staff Evaluation

Heuristic evaluation is an easy method of evaluation that also highlights a large number of issues (Mack & Nielsen, cited in Albion, 1999). The US Department of Health & Human Services (2017) provides information about how to conduct heuristic evaluations. Academic staff can be considered experts in teaching, and as such the author felt that a single response from an academic was sufficient for the purposes of this research.

A member of staff who is familiar with the Cyber Security Fundamentals unit, and has significant experience in teaching, was asked to evaluate the application using a similar process to the students, but with some different aspects of the application utilised and some changes to the questionnaire which they were asked to complete. As per the student evaluation, the staff evaluation was designed to establish how useful they thought the e-learning environment would be for use in the classroom when teaching children.

Both the instructions and the survey were provided electronically, allowing the staff evaluation to be completed at a time that suited the staff member. The participant was asked to fill out a consent form prior to participating. Both the consent form and provided guidance material is available in Appendix E: Evaluation Forms.

5.2.2.1 Methods

An eligible staff member was identified per the requirements in Section 3.3.5.2 Staff Participation Requirements. The identified staff member was required to fill out a consent form prior to starting the evaluation, and evaluation materials were provided remotely allowing the evaluation to be taken at the convenience of the staff member. The evaluation materials consisted of a document with a series of tasks which the staff member was required to undertake before completing a survey which was also provided in the information pack. This pack is available in Appendix E: Evaluation Forms.

The staff member was issued with a participant ID, a username and password to access the application which was randomly assigned from the pool of test accounts which had been generated during the development testing process.

As with the student evaluation, the questionnaire was constructed using the free popular online survey tool, Survey Monkey (2017). This allowed the full evaluation process to take place remotely. The staff member was asked to enter their name into the survey, but was not asked any other personally identifiable information. There was a mix of quantitative and qualitative questions within the questionnaire, as discussed in Section 2.5 Methods of Collection and Analysis of Data. This allowed for the heuristic evaluation questions to be asked, as well as allowing for open-ended information to be obtained to more accurately get their opinion on the e-learning system.

As with the student evaluation, the staff evaluation's closed questions used a modified version of the Likert scale which incorporated a "n/a" option as well as the traditional scale of "Strongly Agree" to "Strongly Disagree".

The questions focussed around the application's usability, and the quality of the learning resources as analysis from the literature review (Section 2) and requirements analysis (Section 3.3) identified these two areas as important to the success of an e-learning environment. The full questionnaire can be seen in Appendix E: Evaluation Forms.

5.2.2.2 Results

The results were collected towards the end of the project alongside the student evaluations. Two secondary school teachers took part in the evaluation. Two teachers were deemed appropriate for the staff analysis as teachers can be considered as experts in teaching and as such a pseudo-heuristic analysis was conducted in combination with a survey. All results from the questionnaire can be seen in Appendix F: Results. The questions asked to teaching staff focussed around hypothesis three (See Section 1.2.3 Hypotheses) in determining the likelihood of the developed resource helping teachers in their delivery of the curriculum.

As with the majority of student evaluators, the teacher found the application both very easy to use and navigate. The teacher strongly agreed that they liked the text based resources. This is interesting as the mean student rating was "Agree". A comparison of the two evaluators' feedback on text-based resources is provided in Figure 5.c.

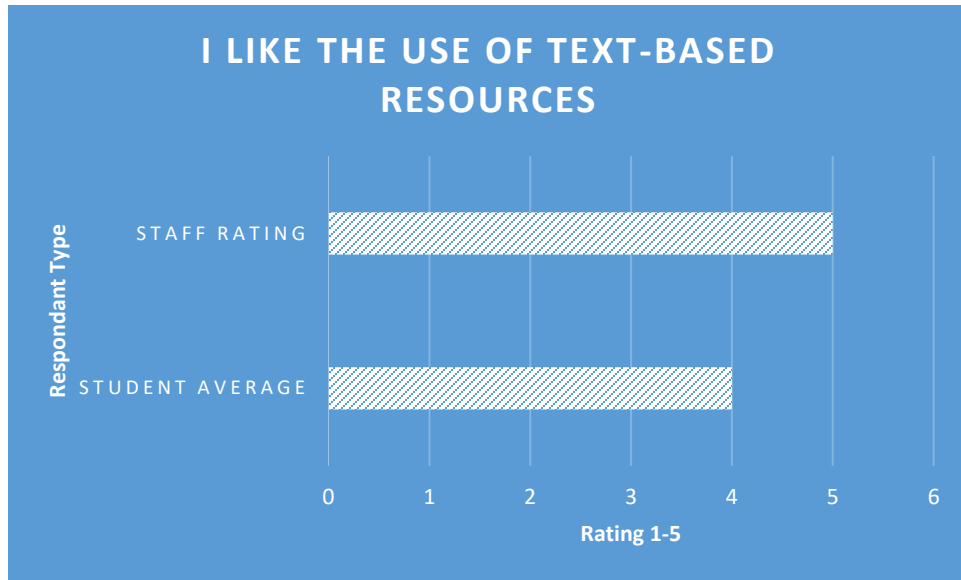


Figure 5.c: Comparison of Staff vs Student Views of Text-Based Resources

Indeed, the staff member generally rated the audio-visual educational resources lower than the text-based resources, contrary to the ratings which the students gave the resources. This is illustrated in Figure 5.d.

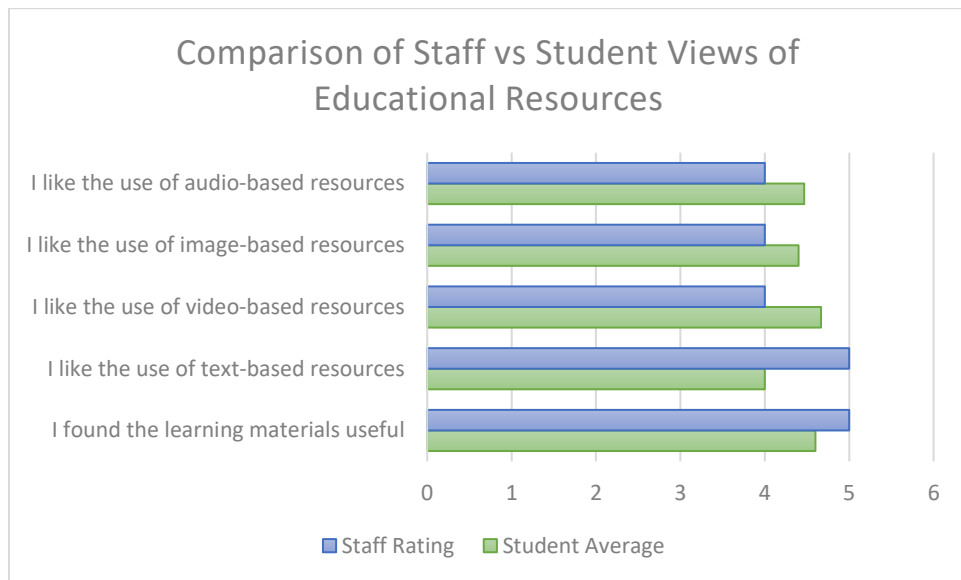


Figure 5.d: Comparison of Staff vs Student Views of Resources

Part of the reason that the teacher may have marked the video-based resources as “Agree” rather than “Strongly Agree” is the use of non-British English in some of the videos. This conclusion is made as the teacher added a comment stating that there should be more British English speakers. Many of the videos used in the prototype had American and other English speakers, and the accents may make it harder for students to learn than accents that they are more used to.

As with the students, the teacher has indicated that more interactive elements within the e-learning environment would engage students better, but even in its current state, the teacher indicated that they could see the environment being used in schools to deliver the cyber security curriculum.

5.3 Conclusions

A large amount of data was generated during the testing and evaluation phase of the project. This was analysed to attempt to answer the research question and to prove the project's hypotheses. From the results gathered, it appears that the introduction of an e-learning environment within secondary schools to deliver the cyber security curriculums could prove very effective. The results are discussed in more detail in the final section of this report.

6 Discussions and Conclusions

This section discusses the results of the project and brings the report to a conclusion. It starts by summarising the project before discussing the results and the potential consequences for the results in relation to the research question and hypotheses. This section also discusses some limitations with the project and where future work could be conducted to build on the research that this project has initiated.

6.1 Project Summary

There is a global cyber security workforce crisis, with a shortage of two million experts across the globe (SQA, 2015a). The Scottish Government have attempted to combat this by introducing a cyber security curriculum into secondary schools. There is a lack of resources for teachers delivering the curriculum as text books are out of date before they are even published (Oxford Cambridge and RSA Examinations, 2014), and teachers do not have the necessary ICT skills (Fernández-Cruz & Fernández-Díaz, 2016). As such, teachers are struggling to deliver the SQA's Cyber Security Fundamentals curriculum effectively.

E-learning is widely used in higher education, but has only started being used in secondary education in recent years (Henley, 2009). Scotland is a world pioneer in the usage of e-learning at the secondary level with the introduction of the Glow Connect platform in 2007, but the platform does not currently deliver the cyber security curriculums effectively. Through the following research question, this project aimed to see if e-learning can help in the delivery of the cyber security curriculums across Scotland:

“Would the development of an e-learning environment for the SQA's Cyber Security Fundamentals unit improve students' understanding of cyber security and increase their abilities in the subject?”

Based upon the research question, the project aimed to evaluate the effectiveness of e-learning in delivering the cyber security curriculum in secondary schools. This was achieved through the Develop and Test research methodology by developing a comprehensive e-learning environment along with some learning resources based on the Cyber Security Fundamentals curriculum.

Akker *et al.* (1999, p. 4) explain that more develop and test style research needs to be conducted, and that this should particularly include work around designing learning environments. They argue that the research should not focus merely on theory, but on whether the developed project works.

The e-learning environment and its learning content was developed by formulating requirements after interviews with both school teachers and staff from the SQA. Upon completion of the e-learning system, two evaluations were carried out to test the research question. One evaluation focussed on the school children and how useful they found the e-learning environment in improving their knowledge of cyber security, and the other evaluation focussed on the school teachers' perspectives. There were two main hypotheses within the project that the two methods of evaluation have helped to answer. These were:

Hyp1: The developed online resource will help students to further their learning of the Cyber Security Curriculum.

Hyp2: The resulting online resource will help teachers to better deliver the Scottish Cyber Security Curriculum.

The use of a combined evaluation allowed the researcher to obtain data from both of the application's main user groups: teachers who are experts in the field of teaching; and students who would utilise the application throughout their learning; in order to satisfy the hypotheses and answer the research question. An analysis of the project in relation to the research question and hypotheses is given in the following section.

6.2 Final Discussion of Results

The main aim of this project was to evaluate the potential benefits of e-learning in delivering cyber security qualifications within secondary level education. The project hypothesised that the delivery of content via an electronic method would help both students and teachers through the learning process, as students would benefit from knowledge imparted directly from the cyber security experts who create the content, and teachers would benefit from having additional resources to help in their teaching.

The research has found that both students and teachers think that the e-learning system could greatly benefit their learning experience in relation to cyber security.⁸ With 93.33% of students either agreeing or strongly agreeing that the application is easy to navigate, and 93.33% agreeing or strongly agreeing that the learning materials are useful, it is clear that the sample of students evaluated value the e-learning environment and believe that it could have benefits on their educational experience. Interestingly, the average quiz score for students was also 93.33%, showing a very good understanding of the curriculum areas covered. Statistically, participants with no knowledge of security whatsoever should have scored 25% in the multi-choice quiz, and with no candidate scoring below 75%, it means that each participant learned something from the e-learning environment.

Students generally found the mix of media to be appealing, and found the use of audio-visual methods better than text-based resources. This is contrary to the teacher's views, suggesting that there may be a conflict between the methods that teachers prefer and the methods which are better for students.

It is not possible with the quantity of data gathered to determine the exact extent to which the e-learning resource could improve students' understanding of the subject without undertaking a far more timely and in-depth analysis with control groups. However, the results do indicate that the resource is likely to have a strong positive impact in the learning experience based on the results from both teachers and students.

⁸ See Section 6.3 Project Limitations for a discussion on the validity of the results based on the sample size used within the evaluation.

6.3 Project Limitations

The results of this project support the hypotheses posed by the author. There are a number of limitations on the project however, which means that further research should be conducted before the results can be confirmed as truly valid.

As mentioned in Section 5.2.1 Student Evaluation, a small sample size was used for the student evaluation. The results from the student evaluation provide an indicative result of what the wider population may find with the e-learning environment, but the evaluation should be carried out on a larger sample in order to fully determine whether the e-learning environment does effectively teach the cyber security curriculum.

In order to achieve a 95% confidence level with a 5% margin of error, 80% of the current population studying the Cyber Security Fundamentals Unit would need to be surveyed. Obtaining an 80% response rate even in future work is likely unfeasible, and as such more realistic work would utilise a sample of at least 31 students but leave a 15% margin of error at the 95% confidence interval (Raosoft, 2004).

The project was conducted over a relatively short timeframe, and as such there are a number of features which were not added to the e-learning environment for the current prototype. Both review of the available literature, and the students' responses to the evaluations indicate that gamification should be included to further engage the students in the e-learning process and better enhance the learning experience.

The developed e-learning system is a prototype application and as such, both the system itself and the learning content are incomplete. Learning materials for all units of the curriculum would need to be produced before the system could be used in schools, as well as an easy method for school administrators to register students.

6.4 Future Work

As discussed in the previous section, there are a number of limitations on the project which leave areas for future work to be undertaken in relation to the project. Some of the features and areas to investigate in the future are outlined in the following subsections.

6.4.1 Gamification

Both the literature review and questionnaire results have highlighted the need for gamification in order to fully engage users in the application. As discussed in Section 6.2 Final Discussion of Results, the variety of media currently in the e-learning environment was found to be engaging to users, but the addition of gamification elements is likely to further improve the user experience.

Hunter (2016) proposed an inter-school leader board in the application. This is one element which could encourage participation due to the competition between schools. It may also encourage students to help each other with their learning in order to improve the school's ranking and promote a group learning ethos.

Each of the e-learning environments evaluated in Section 2.1 Evaluation of Existing E-learning Platforms utilised a badge system to reward users for their efforts. A similar system may encourage individual learning and progress throughout the e-learning environment.

Games in general can be an effective way to get users to learn information without even realising that they are learning. Everson (2014) evaluated one such game by PBS Online (2017) which teaches cyber security basics through an interactive game where the user plays the role of a technology company's Chief Information Security Officer. An interesting area of future research would be to build and integrate full games such as the PBS one into the system to see how it impacts users' engagement and skill levels.

6.4.2 Obtain a Larger Sample for Evaluation

As Discussed in Section 6.3 Project Limitations, the sample size used for this research is not large enough to have a 95% confidence level with a 5% margin of error. Indeed, this research has a 24% margin of error at the 95% confidence level according to the author's calculations. The author recommends that additional research is undertaken with a larger sample size to produce results with a lower margin of error. As previously stated, increasing the number of student participants to 31 students would reduce the error margin by 9%.

Additionally, the role of the teacher in this research was as an expert evaluator. However, a larger sample of teachers and SQA staff could be utilised in further research to obtain additional information from the educator's perspective.

6.4.3 Produce Additional Learning Resources

Section 4.1.2.2 Design of learning materials details the learning resources which have been produced for this research. In order for the e-learning system to be used widely within schools, additional learning resources will need to be created to cover the entire Cyber Security Fundamentals curriculum. This is due to the fact that school teachers would be willing to use an incomplete system with their students.

6.4.4 Expand Research to Evaluate NPAs In Cyber Security

This project has focussed on the SQA's Cyber Security Fundamentals Unit, and how it can be delivered via an online learning system in order to enhance the learning experience. The SQA released three other cyber security curricula at the same time as the Cyber Security Fundamentals Unit – an NPA at SCQF levels 4, 5, and 6. Further research could be conducted to see how e-learning impacts the teaching of these curricula too.

6.4.5 Perform Detailed Analysis Against Learner Types

The development process has focussed very much around the four types of learner identified within Section 2.3, however the evaluation process has focussed on the impact of the learning environment on cyber security education as a whole. An interesting avenue of future research would be to perform further evaluations of the e-learning system against groups of students with known learning style preferences, and see how different learning styles find the e-learning environment. This would allow for the e-learning system to be further refined to find the balance

in educational resources that suits the highest percentage of learners. Additionally, the research found that students and teachers had differing views over which resources were most effective. Another interesting avenue of future research could be to trial different educational methods with different groups of pupils in order to determine the most effective learning methods overall, and see whether this correlates to the methods currently used by teachers.

6.4.6 Conclusions

This project is far from complete and has a lot of further work which could be undertaken in order to further the educational experience of cyber security students in Scotland. By undertaking further work in the areas highlighted above, it could have a wider and more meaningful impact on secondary education within Scotland, and indeed, across the globe.

6.5 Project Conclusions

This project was undertaken to investigate whether cyber security can effectively be taught via e-learning at the secondary school level. Through the analysis of existing e-learning platforms and investigation of common learning types, the author built a robust picture of what an ideal e-learning platform should encompass. The knowledge gained from this review of literature was then used to build an e-learning platform focussed around cyber security for secondary school students.

By developing an e-learning environment which attempts to enhance the learning experience of students undertaking the Cyber Security Fundamentals Unit, as specified by the SQA, the author is attempting to contribute knowledge to society. This knowledge helps to better understand the impact that e-learning can have within secondary level education, and specifically in relation to secondary level cyber security curriculums.

The results from the staff and student evaluations, as well as the students' quiz grades show that the e-learning system has been effective in delivering cyber security information to the students, and that the solution could prove beneficial to both students and teachers if used in schools. This indicates that both hypotheses are true, and answers the research question that this project attempted to answer. However, as discussed in Section 6.3 Project Limitations, it should be noted that a larger sample size is required in order to get a sufficiently low margin of error to be academically sound.

Appendix A: References

AKKER, J., BRANCH, R., GUSTAFSON, K. and PLOMP, T., 1999. *Design Approaches and Tools in Education and Training*. 1st ed. Netherlands: Springer Netherlands.

ALBION, P.R., 1999. *Heuristic evaluation of educational multimedia: from theory to practice*. [unpublished research]. Research ed. Available from: <https://core.ac.uk/download/pdf/11039639.pdf>.

ALLEN, I.E. and SEAMAN, C.A., 2007. Likert Scales and Data Analyses. *Quality Progress*. **40**(7), pp. 64-65.

BALLIAUW, M., 2013. Using GitHub without leaving PhpStorm *WebStorm & PhpStorm Blog* [online]. [viewed 30 March 2017]. Available from: <https://blog.jetbrains.com/webide/2013/02/using-github-without-leaving-phpstorm/>.

BARATA, G., S. GAMA, J. JORGE and D. GONÇALVES., 2013. So Fun It Hurts – Gamifying an Engineering Course. In: SCHMORROW, D. and FIDOPIASTIS, C., eds. *Foundations of Augmented Cognition*. Las Vegas, USA., 2013. Berlin, Heidelberg: Springer, pp.639-648.

BATURAY, M.H. and BIRTANE, M., 2013. *Responsive Web Design: A New Type of Design for Web-based Instructional Content*. , 10 December 2013, Available from: <http://www.sciencedirect.com/science/article/pii/S1877042813048829> ISBN 1877-0428. DOI <http://dx.doi.org/10.1016/j.sbspro.2013.12.259>.

BEACH, J., 2017. *Syntax Highlight Code In Word Documents* [online]. Beach, Jamie. [viewed 12 March 2017]. Available from: <http://planetb.ca/syntax-highlight-word>.

Bootstrap, n.d. *Bootstrap: The world's most popular mobile-first and responsive front-end framework* [online]. [viewed 30 March 2017]. Available from: <http://getbootstrap.com/>.

Cabinet Office, 2016. *The UK Cyber Security Strategy 2011-2016*. London, UK: Cabinet Office. [viewed 23 January 2017]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

CAMPOS, E., 2017. Cyber Security Fundamentals Interactive Learning Environment [email]. EVERSON, T. tevers200@caledonian.ac.uk. 10 February.

CATLIN, H., WEIZENBAUM, N. and EPPSTEIN, C., 2015. *Sass Basics* [online]. Sass. [viewed 30 March 2017]. Available from: <http://sass-lang.com/guide>.

CHANDLER, P. and SWELLER, J., 1991. Cognitive Load Theory and the Format of Instruction. *Cognition and Instruction* [online]. **8**(4), pp. 293-332.

CHEN, L. and TAO, L., 2012. Teaching Web Security using Portable Virtual Labs. *Journal of Educational Technology & Society*. **15**(4), pp. 39.

CHERWINKA, J., 2012. Database Notations tap the full power of Visio *Office Blogs* [online]. [viewed 31 March 2017]. Available from: <https://blogs.office.com/2012/10/24/database-notations-tap-the-full-power-of-visio/>.

CHO, V., CHENG, T.C.E. and LAI, W.M.J., 2009. The role of perceived user-interface design in continued usage intention of self-paced e-learning tools. *Computers & Education* [online]. **53**(2), pp. 216-227. [viewed 16 February 2017]. Available from: <http://dx.doi.org/10.1016/j.compedu.2009.01.014>.

CHUNG, W., CHEN, H., CHANG, W. and CHOU, S., 2006. Fighting cybercrime: a review and the Taiwan experience. *Decision Support Systems*. **41**(3), pp. 669-682.

Codecademy, 2017. *Codecademy* Codecademy. [viewed 23 January 2017]. Available from: <https://www.codecademy.com/>.

Cyber Security Challenge, 2017. *Schools - Cyber Security Challenge UK* [online]. Cyber Security Challenge UK. [viewed 13 February 2017]. Available from: <https://cybersecuritychallenge.org.uk/education/schools>.

Cyber Security Challenge, 2016a. *Challenge Founder Awarded OBE* [online]. Cyber Security Challenge. [viewed 26 October 2016]. Available from: <https://cybersecuritychallenge.org.uk/challenge-founder-awarded-obe/>.

Cyber Security Challenge, 2016b. *Schools* [online]. Cyber Security Challenge. Available from: <https://cybersecuritychallenge.org.uk/education/schools>.

Cybersecurity Excellence Awards, 2016. *Cybersecurity Company Awards - Winners and Finalists* [viewed 23 January 2016]. Available from: <http://cybersecurity-excellence-awards.com/2016-cybersecurity-company-awards/>.

Cybrary, 2017. *Members - Cybrary* [online]. Cybrary. [viewed 06 February 2017]. Available from: <https://www.cybrary.it/members/>.

Cybrary, 2016. *About - Cybrary* Cybrary. [viewed 23 January 2017]. Available from: <https://www.cybrary.it/about/>.

DAVITT, J. 2006. Digital networks: Scotland wakes up with a healthy Glow: Next year will see the launch of a project that aims to provide online resources and joined-up learning for every pupil and teacher in Scotland. *The Guardian (London, England)* [online]. 19 September. [viewed 12 October 2016]. Available from: <http://search.proquest.com.gcu.idm.oclc.org/docview/246568209?accountid=15977>.

DE SÁ, M. and L. CARRIÇO., 2006. Low-fi Prototyping for Mobile Devices. In: Anonymous *CHI '06 Extended Abstracts on Human Factors in Computing Systems*. Montréal, Canada., 2006. New York, USA: ACM, pp.694-699.

DETERDING, S., D. DIXON, R. KHALED and L. NACKE., 2011. From Game Design Elements to Gamefulness: Defining “Gamification”. In: Anonymous *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*. Tampere, Finland., 2011. New York, USA: ACM, pp.9-15.

DEWEY, J., 1963. *Experience and Education* . Collier Books ed. United States of America: Macmillan Publishing Co., Inc.

DU, W. and WANG, R., 2008. SEED: A Suite of Instructional Laboratories for Computer Security Education. *Journal on Educational Resources in Computing (JERIC)*. **8**(1), pp. 1-24. [viewed 29 October 2016]. Available from: DOI 10.1145/1348713.1348716.

DUNN, R. and DUNN, K., 1979. Learning Styles/Teaching Styles: Should They... Can They... Be Matched?. *Educational Leadership*. **36**(4), pp. 238-244.

DUNN, R. and DUNN, K., 1978. *Teaching Students Through Their Individual Learning Styles: A Practical Approach* United States: Allyn & Bacon.

EBERT, E.S. and CULYER, R.C., 2013. *School: An introduction to education* Wadsworth, USA: Cengage Learning.

E-SKILLS UK, 2013. *Cyber Security Learning Pathways Employer Consultation for England*. London, UK: E-SKILLS UK. [viewed 14 October 2016]. Available from: <https://www.itskillsacademy.org.uk/Site/Cyber%20Security/Documents/130418%20JG%20Cyber%20Report%20JA1Np2.pdf>.

EVANS, K. and REEDER, F., 2010. *A Human Capital Crisis in Cybersecurity USA*: Centre for Strategic & International Studies. [viewed 11 October 2016]. Available from: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100720_Lewis_HumanCapital_WEB_BlKWhiteVersion.pdf.

EVERSON, T., 2016. *The Inaugural Scottish Cyber Security Competition* [online]. Tamar Everson Blog. [viewed 26 October 2016]. Available from: <https://tamareverson.co.uk/blog/articles/27/the-inaugural-scottish-cyber-security-competition>.

EVERSON, T., 2014. *A Game About Cats... And Cyber Security* [online]. Tamar Everson Blog. [viewed 16 April 2017]. Available from: <http://tamareverson.co.uk/blog/articles/8/a-game-about-cats-and-cyber-security>.

Facing History and Ourselves, 2016. *Chunking* [online]. Facing History and Ourselves Charity. [viewed 08 April 2017]. Available from: <https://www.facinghistory.org/resource-library/teaching-strategies/chunking>.

FELDER, R., 1988. How students learn: adapting teaching styles to learning styles. In: GRAYSON, L. and BIEDENBACH, J., eds. *Frontiers in Education Conference*. Santa Barbara., 1988. Santa Barbara: IEEE, pp.489-493.

FERNÁNDEZ-CRUZ, F. and FERNÁNDEZ-DÍAZ, M., 2016. Generation Z's Teachers and their Digital Skills. *Comunicar* [online]. **24**(46), pp. 97-105. [viewed 26 October 2016]. Available from: <http://dx.doi.org/10.3916/C46-2016-10>.

FINLEY, K., 2012. *NYU Experiments With Codecademy's Online Hacker Lessons Wired*. [viewed 23 January 2017]. Available from: <https://www.wired.com/2012/09/nyu-teams-up-with-codecademy/>.

FLEMING, N. and BAUME, D., 2006. Learning Styles Again: VARKing up the right tree!. *Educational Developments*.(7.4), pp. 4-7.

GILAKJANI, A., 2012. Visual, Auditory, Kinaesthetic Learning Styles and Their Impacts on English Language Teaching. *Journal of Studies in Education* [online]. **2**(1), pp. 104-113. [viewed 02 February 2017].

Github, 2017. *Features For Collaborative Coding* [Online]. Github. [viewed 30 March 2017]. Available from: <https://github.com/features#project-management>.

GONZÁLEZ, C., 2010. What do university teachers think eLearning is good for in their teaching?. *Studies in Higher Education* [online]. **31**(1), pp. 67-78.

GOSLER, J., 2010. *Cyberwarrior Shortage Threatens U.S. Security*. NPR News, 19 July 2010.

GUBA, E. and LINCOLN, Y., 1989. *Fourth Generation Evaluation* California, USA: Sage.

HENLEY, B.F., 2009. *Developing eLearning: A case study of Tennessee High School*. PhD dissertation, East Tennessee State University. [viewed 22 October 2016]. Available from: <http://search.proquest.com/docview/304874653?accountid=15977>.

HM Government., 1998. *Data Protection Act 1998*.

HUNTER, S., 2016. Telephone Interview [telephone interview]. EVERSON, T. 24 October.

Information Commissioner's Office, 2012. *Report on the data protection guidance we gave schools in 2012*. Cheshire, UK: Information Commissioner's Office. [viewed 18 April 2017]. Available from: <https://ico.org.uk/media/action-weve-taken/self-assessments/2790/report-dp-guidance-for-schools.pdf>.

- IQBAL, R., et al., 2005. User-centred Design and Evaluation of Ubiquitous Services. In: *Anonymous Proceedings of the 23rd annual international conference on Design of communication: documenting & designing for pervasive information*. Coventry, United Kingdom., 2005. New York, USA: ACM New York, pp.138-145.
- IRISH, P. and MANIAN, D., 2013. *HTML5 Readiness* [online]. HTML5 Readiness. Available from: <http://html5readiness.com/>.
- JOHNSON, D. and WILES, J., 2003. Effective affective user interface design in games. *Ergonomics* [online]. **46**(13-14), pp. 1332-1345. [viewed 06 February 2017]. Available from: <http://dx.doi.org/10.1080/00140130310001610865>.
- KALYUGA, S., CHANDLER, P. and SWELLER, J., 2004. When redundant on-screen text in multimedia technical instruction can interfere with learning. *Human Factors*. **46**(3), pp. 567-581.
- KANGAS, E. and KINNUNEN, T., 2005. Applying User-Centered Design to Mobile Application Development. *Communications of the ACM - Designing for the Mobile Device* [online]. **48**(7), pp. 55-59. [viewed 30 March 2017]. Available from: 10.1145/1070838.1070866.
- KANTNER, L. and S. ROSENBAUM., 1997. Usability Studies of WWW Sites: Heuristic Evaluation vs. Laboratory Testing. In: *Anonymous Proceedings of the 15th Annual International Conference on Computer Documentation*. Salt Lake City, Utah, USA., 1997. ACM New York, pp.153-160.
- KEEN, B., 2016. *generatedata.com* [online]. generatedata.com. [viewed 20 January 2017]. Available from: <http://www.generatedata.com>.
- Khan Academy, 2017. *Khan Academy* Khan Academy. [viewed 23 January 2017]. Available from: <https://www.khanacademy.org>.
- KHAN, B.H., 2005. *Managing e-learning: Design, delivery, implementation, and evaluation* IGI Global.
- LAVIN, P., 2006. *Object-Oriented PHP: Concepts, Techniques, and Code* San Fransico, USA: No Starch Press.
- LEE, M. and A. KO., 2015. Comparing the Effectiveness of Online Learning Approaches on CS1 Learning Outcomes. In: *Anonymous Proceedings of the eleventh annual International Conference on International Computing Education Research*. Omaha, Nebraska., 2015. Omaha, Nebraska: ACM, pp.237-246.
- LIAW, S., HUANG, H. and CHEN, G., 2007. Surveying instructor and learner attitudes toward e-learning. *Computers & Education*. **49**(4), pp. 1066-1080.

MA, H., 2013. Tech Services on the Web: Codecademy; <http://www.codecademy.com/>. *Technical Services Quarterly* [online]. **30**(3), pp. 338-339. [viewed 23 January 2017]. Available from: 10.1080/07317131.2013.788372.

MACGREGOR, A. and ELLIOT, B., 2016. Interview at SQA [interview]. EVERSON, T. 3 November.

MANDINACH, E., 2005. The Development of Effective Evaluation Methods for E-Learning: A Concept Paper and Action Plan. *Teachers College Record* [online]. **107**(8), pp. 1814-1835. [viewed 07 February 2017].

ManpowerGroup, 2015. *2015 Talent Shortage Survey*. ManpowerGroup. [viewed 30 March 2017]. Available from: http://www.manpowergroup.com/wps/wcm/connect/db23c560-08b6-485f-9bf6-f5f38a43c76a/2015_Talent_Shortage_Survey_US-lo_res.pdf?MOD=AJPERES.

MARSHALL, S., 2007. Engagement Theory, WebCT, and Academic Writing in Australia. *International Journal of Education and Development using Information and Communication Technology*. **3**(2), pp. 109-115.

MCGETTRICK, A., 2017. Cyber Security Education: Research [email]. EVERSON, T. tamar.everson@gcu.ac.uk. 23 January.

Microsoft, 2016a. *Project Management* [online]. Microsoft. [viewed 22 January 2017]. Available from: <https://www.visualstudio.com/en-us/docs/work/guidance/cmml/guidance-project-management>.

Microsoft., 2016b. *Project Management*. [online image]. [viewed 22 January 2017]. Available from: <https://msdn.microsoft.com/en-us/library/ee461565.aspx>.

MIESSLER, D., 2014. *SecLists/10k_most_common.txt* GitHub. [viewed 10 December 2016]. Available from: https://github.com/danielmiessler/SecLists/blob/master/Passwords/10k_most_common.txt.

MOGHADDAM, G. and MOBALLEGHI, M., 2008. How Do We Measure Use of Scientific Journals? A Note on Research Methodologies. *Scientometrics*. **76**(1), pp. 125-133.

MOHONEY, D., 2011. Wanted: Cybersecurity personnel. *Urgent Communications* [online]. **29**(3), pp. 16-22. [viewed 11 October 2016]. Available from: <http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=59414386&S=R&D=bsh&EbscoContent=dGJyMMvl7ESep7I4zOX0OLCmr06ep7NSsay4TLswxWXS&ContentCustomer=dGJyMPGutky3rq9NuePfgex44Dt6fIA>.

MORRISON, B. and B. DISALVO., 2014. Khan Academy Gamifies Computer Science. In: DOUGHERTY, J., NAGEL, K., DECKER, A. and EISELT, K., eds. *Proceedings of the 45th*

ACM technical symposium on Computer science education. Atlanta, Georgia, USA., 2014. New York, USA: ACM, pp.39-44.

New Digital Group, 2017. *All About Smarty* [online]. New Digital Group. [viewed 30 March 2017]. Available from: http://www.smarty.net/about_smarty.

NIELSEN, J. and R. MOLICH., 1990. Heuristic Evaluation of User Interfaces. In: Anonymous *Proceedings of the SIGCHI Conference on Human Factors in Computing*. Seattle, USA., 1990. USA: ACM New York, pp.249-256.

NOWILL, R., 2014. *Identifying, inspiring and enabling new cyber security talent*. [online]. UK: Cyber Security Challenge. [viewed 26 October 2016]. Available from: <https://cybersecuritychallenge.org.uk/wp-content/uploads/2014/07/IISP-PulseMay14-CyberSecurityChallenge.pdf>.

O'CONNOR, T., et al., 2014. *HTML5*. [online]. online: W3C., [viewed 08 April 2017]. Available from: <https://www.w3.org/TR/html5/>.

OLSSON, M. and P. MOZELIUS., 2016. On Design of Online Learning Environments for Programming Education. In: Anonymous *European Conference on e-Learning*. Kidmore End, United Kingdom., 2016. Kidmore End, United Kingdom: Academic Conferences International Limited, pp.533-539.

Oracle Corporation, 2017. *MySQL* [online]. Oracle Corporation. [viewed 30 March 2017]. Available from: <https://www.mysql.com/>.

OTTO, M., 2012. Does Twitter use Twitter Bootstrap? *Quora* [online]. [viewed 30 March 2017]. Available from: <https://www.quora.com/Does-Twitter-use-Twitter-Bootstrap/answer/Mark-Otto?srid=4xYn>.

Oxford Cambridge and RSA Examinations, 2014. *Oxford Cambridge and RSA Examinations – Written evidence (DSC001)* [online]. HM Government. [viewed 15 April 2017]. Available from: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-skills-committee/digital-skills/written/11803.html>.

PATTON, M., 2015. *Qualitative Research and Evaluation Methods*. 4th ed. USA: SAGE Publications, Inc. Available from: <https://us.sagepub.com/en-us/nam/qualitative-research-evaluation-methods/book232962#preview>.

PBS Online, 2017. *Cybersecurity Lab* PBS Online. [viewed 16 April 2017]. Available from: <http://www.pbs.org/wgbh/nova/labs/lab/cyber/>.

Raosoft, 2004. *Sample size calculator* Raosoft Inc. [viewed 17 April 2017]. Available from: <http://www.raosoft.com/samplesize.html>.

RAYMER, R., 2011. Gamification: Using Game Mechanics to Enhance eLearning. *eLearn* [online]. **2011**(9), [viewed 16 February 2017]. Available from: 10.1145/2025356.2031772.

ROBERTSON, A., 2015. *Schools to offer qualifications in cyber security* [online]. Dods Parliamentary Communications Ltd. [viewed 25 October 2016]. Available from: <https://www.holyrood.com/articles/news/schools-offer-qualifications-cyber-security>.

ROFFE, I., 2002. E-learning: Engagement, enhancement and execution. *Quality Assurance in Education*. **10**(1), pp. 40-50.

SHATTUCK, S., 2016. The Four Different Types of Learners, And What They Mean to Your Presentations *Prezi* [online]. [viewed 26 January 2017]. Available from: <https://blog.prezi.com/the-four-different-types-of-learners-and-what-they-mean-to-your-presentations-infographic/>.

SQA, 2015a. *Group Award Specification: NPAs in Cyber Security at SCQF level 4 (GK7W 44), Cyber Security at SCQF level 5 (GK7X 45) and Cyber Security at SCQF level 6 (GK7Y 46)*. Scotland, UK: Scottish Qualifications Authority. [viewed 23 October 2016]. Available from: <http://www.sqa.org.uk/sqa/74738.html>.

SQA, 2015b. *Guide To Assessment*. [online]. Glasgow, UK: Scottish Qualifications Authority. [viewed 20 March 2017]. Available from: http://www.sqa.org.uk/files_ccc/Guide_To_Assessment.pdf.

SQA, 2015c. *National Unit Specification: Cyber Security Fundamentals (SCQF level 4)*. [online]. Glasgow, Scotland: Scottish Qualifications Authority. [viewed 18 December 2016]. Available from: <http://www.sqa.org.uk/sqa/files/nu/H9T544.pdf>.

SQA, 2015d. *SQA National Progression Awards - Cyber Security* [video]. 5 October 2015. [viewed 26 October 2016]. Available from: <https://www.youtube.com/watch?v=ENG1YQR118M>.

Statista, 2017a. *Frequency of computer use in the United Kingdom (UK) and European Union (EU-28 countries) in 2015* [online]. Statista. [viewed 26 March 2017]. Available from: <https://www.statista.com/statistics/275251/frequency-of-computer-use-in-the-united-kingdom-uk-and-eu/>.

Statista, 2017b. *Share of individuals who used the computer daily in Great Britain from 2006 to 2015, by age* [online]. Statista. [viewed 26 March 2017]. Available from: <https://www.statista.com/statistics/275996/daily-computer-usage-penetration--in-great-britain-by-age/>.

STEVENSON, A., 2015. e-learning. In: STEVENSON, A. ed., *Oxford Dictionary of English (3 ed.)* Oxford, UK.: Oxford University Press.

STOČES, M., et al., 2015. Cross-Platform User Interface of E-Learning Applications. In: Anonymous *11th International Conference Mobile Learning*. Madeira, Portugal., 2015. International Association for Development of the Information Society, pp.135-138.

Survey Monkey, 2017. *SurveyMonkey: Free online survey software & questionnaire tool* SurveyMonkey. [viewed 13 April 2017]. Available from: <https://www.surveymonkey.co.uk/>.

SWELLER, J., 1999. *Instructional design in technical areas* Camberwell, Australia: ACER Press.

SYAAMANTAK, D. and C. RAJEEV., 2015. A Proposed Systematic User-Interface Design Framework for Synchronous and Asynchronous E-Learning Systems. In: MANDAL, J., et al., ed. *Second International Conference INDIA 2015.*, 2015. New Delhi, India: Springer India, pp.337-347.

Talent LMS., 2014. *E-Learning: Concepts, Trends and Applications* [online]. 1.1st ed. California, USA: Epignosis. [viewed 25 January 2017]. Available from: <https://www.talentlms.com/elearning/elearning-101-jan2014-v1.1.pdf>.

TAYLOR, G., 2005. *Integrating Quantitative and Qualitative Methods in Research*. 3rd ed. USA: University Press of America.

TRINIDAD, O., 2005. *Demographics and Learning Styles of Automotive Technology Students*. Masters of Science, Southern Illinois University. [viewed 27 January 2017]. Available from: <https://books.google.co.uk/books?id=G3Fr1WliGRgC&lpg=PP1&dq=percentage%20of%20read.write%20learners&pg=PP1#v=onepage&q&f=false>.

TURNER, L. 2003. Revision Guide: On the Web Revision. *The Guardian* [online]. 8 April. [viewed 27 October 2016]. Available from: <http://search.proquest.com.gcu.idm.oclc.org/docview/245966143?accountid=15977>.

University of Cambridge, 2015. *Participant information sheets and consent forms* University of Cambridge. [viewed 10 April 2017]. Available from: <http://www.bio.cam.ac.uk/psyres/information sheets>.

US Department of Health & Human Services, 2017. *Heuristic Evaluations and Expert Reviews* [online]. US Department of Health & Human Services. [viewed 11 April 2017]. Available from: <https://www.usability.gov/how-to-and-tools/methods/heuristic-evaluation.html>.

VARAK, 2015. *Research & Statistics* [online]. VARAK. [viewed 03 February 2017]. Available from: <http://vark-learn.com/introduction-to-vark/research-statistics/>.

VIGDERHOUS, G., 1977. The Level of Measurement and “Permissible” Statistical Analysis in Social Research. *Pacific Sociological Review*. **20**(1), pp. 61-72.

VIRZI, R., J. SOKOLOV and D. KARIS., 1996. Usability problem identification using both low- and high-fidelity prototypes. In: Anonymous *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Vancouver, Canada., 1996. New York, USA: ACM, pp.236-243.

VOUTILAINEN, J., J. SALONEN and T. MIKKONEN., 2015. On the Design of a Responsive User Interface for a Multi-device Web Service. In: Anonymous *Proceedings of the Second ACM International Conference on Mobile Software Engineering and Systems*. Florence, Italy., 2015. Piscataway, NJ, USA: IEEE Press, pp.60-63.

WALKER, D. 2007. Learning platforms: The future/resources: We are on the verge of profound change: john Connell: comment: The head of development for Glow, Scotlands new learning platform, explains how they launched a system that will link 800,000 pupils and educators across the country. *The Guardian* [online]. 9 January. [viewed 27 October 2016]. Available from: <http://search.proquest.com/docview/246571203?accountid=15977>.

WALSH, B., 1999. In a nutshell. *Teaching History* [online]. 0(94), [viewed 26 January 2017].

Appendix B: Nomenclature

CSS	Cascade Style Sheet. A language used to present documents written in markup languages.
HTML	HyperText Markup Language. A worldwide language used for displaying websites within web browsers.
HTTP	HyperText Transfer Protocol. A common protocol used for transferring information across the internet.
HTTPS	HTTP over Secure Socket Layer. An encrypted version of HTTP.
MOOC	Massive Open Online Course. A free online course made available to a large number of people.
NPA	National Progression Award. A type of certification offered by the SQA.
PHP	PHP Hypertext Pre-processor. A scripting language often used to create dynamic HTML web pages.
Sass	Syntactically Awesome Style Sheets. An extension to CSS that allows easy updating of styles across an entire project. A type of CSS Pre-processor.
SQA	Scottish Qualifications Authority. The body responsible for accrediting educational awards in Scotland.
SQL	Structured Query Language. A language commonly used to interact with databases.
SSH	Secure Shell. A protocol used to communicate with remote computers securely.
VCS	Version Control System. A tool designed to keep on track of revisions of software.

Appendix C: Related Resources

A number of tools and software have been mentioned throughout this report. Links to further information about each system have been provided in the following table. All links are correct at the time of writing

Software/Resource	Summary	URL
BBC Bitesize	Educational resources for schools provided by the BBC	http://www.bbc.co.uk/education
Blackboard	Commercial Learning Platform	http://blackboard.com
Code School	Commercial online e-learning environment for coding	http://codeschool.com
Codecademy	Free online e-learning environment for coding	https://www.codecademy.com/
Cyber Security Fundamentals National Unit Specification	The SQA's specification document for the Cyber Security Fundamentals curriculum.	http://www.sqa.org.uk/sqa/files/nu/H9T544.pdf
Cybersecurity Lab	A Cyber Security cat game where the player defends a global social media network	http://www.pbs.org/wgbh/nova/labs/lab/cyber/
Cybrary	Free online cyber security training	http://cybrary.it/
Glow Connect	The E-Learning platform used in schools across Scotland managed by Educate Scotland.	https://connect.glowscotland.org.uk/
Guide to Assessment	The SQA's assessment guidance documentation.	http://www.sqa.org.uk/files_ccc/Guide_To_Assessment.pdf
Khan Academy	Free video-based educational resources	http://khanacademy.com/
Moodle	Open Source Learning Platform	https://moodle.org

SEED Environment	Du & Wang's (2008) virtual machine-based environment	http://www.cis.syr.edu/~wedu/seed/instructor_manual.html
Solar	The SQA's online assessment tool.	http://www.sqasolar.org.uk
SWEET Learning Environment	Chen and Tao's (2012) practical educational resources	http://csis.pace.edu/~lchen/sweet/

Appendix D: Email and Interview Sources

This appendix contains transcripts of any emails and interviews which have been undertaken as part of the research.

This page has been redacted to avoid personal information or application source code disclosure. Contact the author if information from this page is required.

This page has been redacted to avoid personal information or application source code disclosure. Contact the author if information from this page is required.

This page has been redacted to avoid personal information or application source code disclosure. Contact the author if information from this page is required.

This page has been redacted to avoid personal information or application source code disclosure. Contact the author if information from this page is required.

This page has been redacted to avoid personal information or application source code disclosure. Contact the author if information from this page is required.

This page has been redacted to avoid personal information or application source code disclosure. Contact the author if information from this page is required.


This page has been redacted to avoid personal information or application source code disclosure. Contact the author if information from this page is required.

This page has been redacted to avoid personal information or application source code disclosure. Contact the author if information from this page is required.

Appendix E: Evaluation Forms

The evaluation forms which have been utilised for this project are available in the below subsections. This includes the student and staff participant information sheet, consent forms, as well as the questionnaires which have been produced as part of the evaluations.

E.1 Staff Information Sheet & Consent Form

	<p>Researcher: Tamar Everson Email: tevers200@caledonian.ac.uk Phone: [Redacted]</p>
---	---

Evaluation of E-learning in Cyber Security: Participant Information Sheet

Invitation

Before you decide to take part in this study, it is important for you to understand why the research is being done and what it will involve. Please read the following information carefully before deciding whether or not to take part. You can discuss it with others, or a member of the research team before making a decision to partake.

Purpose of the study

The Scottish Qualifications Authority recently released a number of cyber security curriculums into Scottish Schools. This study is attempting to determine the effectiveness of e-learning to teach the cyber security curriculum in secondary schools. The study will be completed on 21 April 2017.

Why have you been chosen?

You have been chosen to take part in the study as you work at the SQA and are familiar with the cyber security qualifications. As part of this research, the researcher is obtaining research results from both students and educators to build a complete picture as to the effectiveness of e-learning within the secondary cyber security curriculum.

Do you have to take part?

Participation in this study is completely voluntary, and you can refuse to take part or withdraw from the research now or up until the research is published. If you do choose to withdraw from the study, you will not incur any penalty or loss.

What will happen to me if I take part?

You will be asked to access an online website. This website is a prototype of the e-learning environment that is being developed to deliver the cyber security curriculum. You will be asked to navigate the website and perform some actions whilst on it. A questionnaire will be provided for you to fill in throughout the task in order to obtain data for use in the analysis. You may also be asked some questions in an interview. This interview will be recorded.

What do I have to do?

You will need a computer with internet access in order to complete the study. You will be asked to spend up to 30 minutes using the website and completing the questionnaire.

Figure E.a: SQA Participant Information Form Page 1 of 2



Researcher: Tamar Everson

Email: tevers200@caledonian.ac.uk

Phone: [Redacted]

Risks in Taking Part

There are no foreseeable risks or discomforts in taking part. If you are uncomfortable sitting in front of a computer for the duration of the study, you are free to stop and move around before continuing.

Possible Benefits of Taking Part

The study aims to improve cyber security education delivery within Scotland, and the wider United Kingdom. Participation in this study helps to gather more data to better improve this.

Will my taking part in this project be kept confidential?

All information collected about you over the course of the study will be kept strictly confidential. Personal data will be kept on a secure computer with access only by the immediate research team. Upon completion of the study, your questionnaire results will be anonymised and the original questionnaires destroyed. Your user account on the e-learning website will also be deleted.

What will happen to the results of the research?

The results will be published in the final year honours project for the researcher which is being undertaken at Glasgow Caledonian University. Results may be presented at conferences and written up in journals. If any individual data is presented, it will be totally anonymous with no means of identifying the individuals involved.

Who is organising and funding the research?

Glasgow Caledonian University is undertaking the research.

Ethical Considerations

This project has received ethical approval from Glasgow Caledonian University's School of Engineering and Built Environment Ethics Committee.

Contact for further information

Address: Tamar Everson, Glasgow Caledonian University, G4 0DP, United Kingdom.

Phone: [Redacted]

Email: tevers200@caledonian.ac.uk

Figure E.b: SQA Participant Information Form Page 2 of 2



Researcher: Tamar Everson
Email: tevers200@caledonian.ac.uk
Phone: [Redacted]

Evaluation of E-learning in Cyber Security: Consent Form

I confirm that I have read and understand the Participant Information Sheet

I have had the opportunity to ask questions, and have them answered

I understand that all personal information will remain confidential and that all efforts will be made to ensure that I cannot be identified (except as might be required by law)

I agree that data gathered in this study may be stored anonymously and securely for the duration of this research

I understand that my participation is voluntary and that I am free to withdraw at any time without giving a reason.


I agree to take part in this study

Participant Name:

Participant Signature:

Figure E.c: SQA Participant Consent Form

E.2 Student Information Sheet & Consent Form

	Researcher: Tamar Everson Email: tevers200@caledonian.ac.uk Phone: [Redacted]
---	--

Evaluation of E-learning in Cyber Security: Participant Information Sheet

Invitation

Before you (or your child) decide to take part in this study, it is important for you to understand why the research is being done and what it will involve. Please read the following information carefully before deciding whether or not to take part. You can discuss it with others, or a member of the research team before making a decision to partake.

Purpose of the study

The Scottish Qualifications Authority recently released a number of cyber security curriculums into Scottish Schools. This study is attempting to determine the effectiveness of e-learning to teach the cyber security curriculum in secondary schools. The study will be completed on 21 April 2017.

Why have you been chosen?

You, or your child, has been chosen to take part in the study as they fall into the age range of the students who would be undertaking the new cyber security curriculum. As part of this research, the researcher is obtaining research results from both students and educators to build a complete picture as to the effectiveness of e-learning within the secondary cyber security curriculum.

Do you have to take part?

Participation in this study is completely voluntary, and you can refuse to take part or withdraw from the research now or up until the research is published. If you do choose to withdraw from the study, you will not incur any penalty or loss.

What will happen to me if I take part?

You will be asked to access an online website. This website is a prototype of the e-learning environment that is being developed to deliver the cyber security curriculum. You will be asked to navigate the website and perform some actions whilst on it. A questionnaire will be provided for you to fill in throughout the task in order to obtain data for use in the analysis.

What do I have to do?

You will need a computer with internet access in order to complete the study. You will be asked to spend up to 30 minutes using the website and completing the questionnaire.

Risks in Taking Part

There are no foreseeable risks or discomforts in taking part. If you are uncomfortable sitting in front of a computer for the duration of the study, you are free to stop and move around before continuing.

Figure E.d: Student Participant Information Form Page 1 of 2



Researcher: Tamar Everson

Email: tevers200@caledonian.ac.uk

Phone: [Redacted]

Possible Benefits of Taking Part

The study aims to improve cyber security education delivery within Scotland, and the wider United Kingdom. Participation in this study helps to gather more data to better improve this.

Will my taking part in this project be kept confidential?

All information collected about you over the course of the study will be kept strictly confidential. Personal data will be kept on a secure computer with access only by the immediate research team. Upon completion of the study, your questionnaire results will be anonymised and the original questionnaires destroyed. Your user account on the e-learning website will also be deleted.

What will happen to the results of the research?

The results will be published in the final year honours project for the researcher which is being undertaken at Glasgow Caledonian University. Results may be presented at conferences and written up in journals. If any individual data is presented, it will be totally anonymous with no means of identifying the individuals involved.

Who is organising and funding the research?

Glasgow Caledonian University is undertaking the research.

Ethical Considerations

This project has received ethical approval from Glasgow Caledonian University's School of Engineering and Built Environment Ethics Committee.

Contact for further information

Address: Tamar Everson, Glasgow Caledonian University, G4 0DP, United Kingdom.

Phone: [Redacted]

Email: tevers200@caledonian.ac.uk

Figure E.e: Student Participant Information Form Page 2 of 2



Researcher: Tamar Everson
Email: tevers200@caledonian.ac.uk
Phone: [Redacted]

Evaluation of E-learning in Cyber Security: Consent Form

If the participant is under the age of 18, the parent or guardian must fill out this form:

I confirm that I have read and understand the Participant Information Sheet

I have had the opportunity to ask questions, and have them answered

I understand that all personal information will remain confidential and that all efforts will be made to ensure that I cannot be identified (except as might be required by law)

I agree that data gathered in this study may be stored anonymously and securely for the duration of this research

I understand that my participation is voluntary and that I am free to withdraw at any time without giving a reason.

<p>To be filled in by the participant</p> <p>I agree to take part in this study <input type="checkbox"/></p> <p>Participant Name: <input type="text"/></p> <p>Participant Signature: <input type="text"/></p>	<p>If the participant is under 18 years of age, the parent or guardian must also fill in the following section:</p> <p>I agree that my child can take part in this study <input type="checkbox"/></p> <p>Parent/Guardian Name: <input type="text"/></p> <p>Child Name: <input type="text"/></p> <p>Parent/Guardian Signature: <input type="text"/></p>
--	--

Figure E.f: Student Participant Consent Form

E.3 Staff Worksheet



Researcher: Tamar Everson

Email: tevers200@caledonian.ac.uk

Phone:

Evaluation of E-learning in Cyber Security: Participant Worksheet

Introduction

Thank you for agreeing to take part in this research. Please follow the instructions below in order to complete the research. You will be asked to visit a prototype website which is designed to teach students the cyber security curriculum which has recently been brought into Scottish Schools.

Please note that some pages have very little content as they were not deemed necessary for the purposes of this study. If you think that any important content is missing from the prototype, however, please make a note of this in the final survey.

Methods

1. Please visit the following website: www.ethicalhacking.org.uk
2. You will need to enter the following username and password to view the site:
 - Username: honours
 - Password: honours
3. When you visit the site you will be brought to the homepage. Please click the login button to login. You will need the following username and password to view the site:
 - Username: {username}
 - Password: {password}
4. Take a few minutes to look through the website and familiarise yourself with it.
5. Navigate to the “Chapters” page
6. Click on Chapter 1: Security Measures to Help Reduce Vulnerabilities and Threats, then on Page 1: Password Strength
7. Take a look at some of the teaching materials provided
8. When you reach the quiz page, take a look at the questions. You do not need to do the quiz as the teacher role.
9. After this, browse to the “My Users” page of the application and click “St. Andrew's Secondary”. Click on one of the users (suggested either “Tamar Everson” or “Priscilla Hughes” as both have multiple quiz attempts), and then on “View Grades” on that users’ profile page. Note that you can view the grades and the individual questions the user got right and wrong.
10. After you have completed the above steps, please browse to the following website and complete a short questionnaire. You will need to enter your participant number. This number will be used to identify your result should you wish to withdraw from the study before the results are published as detailed in the participant summary documentation.
 - Participant ID: {id}
 - URL: <https://www.surveymonkey.co.uk/r/ZYG75TV>
11. That’s it. Thank you for your participation.

E.4 Student Worksheet



Researcher: Tamar Everson

Email: tevers200@caledonian.ac.uk

Phone:

Evaluation of E-learning in Cyber Security: Participant Worksheet

Introduction

Thank you for agreeing to take part in this research. Please follow the instructions below in order to complete the research. You will be asked to visit a prototype website which is designed to teach students the cyber security curriculum which has recently been brought into Scottish Schools.


Please note that some pages have very little content as they were not deemed necessary for the purposes of this study. If you think that any important content is missing from the prototype, however, please make a note of this in the final survey.

Methods

1. Please visit the following website: www.ethicalhacking.org.uk
2. You will need to enter the following username and password to view the site:
 - Username: honours
 - Password: honours
3. When you visit the site you will be brought to the homepage. Please click the login button to login. You will need the following username and password to view the site:
 - Username: {username}
 - Password: {password}
4. Take a few minutes to look through the website and familiarise yourself with it.
5. Navigate to the “Chapters” page
6. Click on Chapter 1: Security Measures to Help Reduce Vulnerabilities and Threats
7. Click on Page 1: Password Strength
8. Start working through the learning content provided. Follow through each page of learning material in the chapter until you get to the quiz. Note that you do not have to read all of the learning resources on every page, but enough to get a feel for the content.
9. When you reach the quiz page, attempt the quiz and proceed to view your results.
10. After this, browse to the “My Grades” page of the application and view your grades.
11. After you have completed the above steps, please browse to the following website and complete a short questionnaire. You will need to enter your participant number. This number will be used to identify your result should you wish to withdraw from the study before the results are published as detailed in the participant summary documentation.
 - Participant ID: {id}
 - URL: <https://www.surveymonkey.co.uk/r/ZW57BD9>
12. That’s it. Thank you for your participation.

E.5 Staff Questionnaire

Staff Evaluation


1. Please enter your participant ID 

2. If you had any issues completing the previous section of the exercise (using the website) then please detail these here. 


Next

Figure E.g: Staff Questionnaire Page 1


Staff Evaluation


3. The following questions are about your general usage of the application 

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	N/A
I found the application easy to log into	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I found the application easy to navigate	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4. The following questions are about the learning resources 

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	N/A
I think that the learning materials will help students in their understanding of the curriculum	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I like the use of text-based resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I like the use of video-based resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I like the use of image-based resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I like the use of audio-based resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>


5. Is there any type of resource that you would like to see more of? 


6. The following questions relate to the system's usage in schools 


	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	N/A
I think that the system would help students to better understand cyber security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I can see this being used in schools	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Teachers would find this resource useful in delivering the cyber security curriculum	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Students would find this resource useful when learning about cyber security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>


Figure E.h: Staff Questionnaire Page 2

Staff Evaluation

7. What features (if any) would you like to be added to the system, and why? 

8. What features (if any) would you like to be removed to the system, and why? 

9. Are there any other improvements that you think should be made to the solution? 


10. Do you have any other comments? 


[Prev](#) [Done](#)

Figure E.i: Staff Questionnaire Page 3

E.6 Student Questionnaire

Student Evaluation

1. Please enter your participant ID 

2. If you had any issues completing the previous section of the exercise (using the website) then please detail these here. 

Next

Figure E.j: Student Questionnaire Page 1

Student Evaluation

* 3. The following questions are about your general usage of the application 

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	N/A
I found the application easy to log into	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I found the application easy to navigate	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* 4. The following questions are about the learning resources 

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	N/A
I found the learning materials useful	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I like the use of text-based resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I like the use of video-based resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I like the use of image-based resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I like the use of audio-based resources	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. Is there any type of resource that you would like to see more of? 

* 6. The following questions relate to the system's usage in schools 


	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	N/A
I think that using this system would help me to better understand cyber security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I can see my teacher asking me to use a resource like this	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
By using this, I would learn more about cyber security than I would without it?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>


Prev


Next

Figure E.k: Student Questionnaire Page 2

Student Evaluation

7. What features (if any) would you like to be added to the system, and why? 

8. What features (if any) would you like to be removed to the system, and why? 

9. Are there any other improvements that you think should be made to the solution? 


10. Do you have any other comments? 

Figure E.1: Student Questionnaire Page 3

Appendix F: Results

F.1 Student Evaluation Results

The results from each question in the student evaluation are listed below. Quantitative question results are given in both a frequency table and a bar chart. Qualitative question results are presented in a table. There were fifteen respondents in total.

F.1.1 Question 1

Question 1 asked participants for their participant ID. This was in order to identify responses should a participant ask to withdraw from the study. It was a compulsory question. The results can be seen in Table F.a.

Table F.a: Student Question 1 Results

Please enter your participant ID
74802
87419
80192
99313
68321
32784
62637
44553
51259
33854
33461
51269
18007
10904
91836

F.1.2 Question 2

Question 2 asked participants to detail any issues that they had when using the application prior to the survey. It was an optional question and received two responses. The results can be seen in Table F.b.

Table F.b: Student Question 2 Results

If you had any issues completing the previous section of the exercise (using the website) then please detail these here.
password reset function did not work
The flow chart on chapter 1, page 1 could be clearer. The green diamonds made it a bit confusing as they stopped the flow of the arrows.

F.1.3 Question 3

Question three asked participants about how easy or difficult they found the application to use. It was a compulsory question. The results can be seen in Table F.c and Figure F.a.

Table F.c: Student Question 3 Results

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Average
I found the application easy to log into	2	0	0	4	9	15	4.2
I found the application easy to navigate	1	0	0	4	10	15	4.467

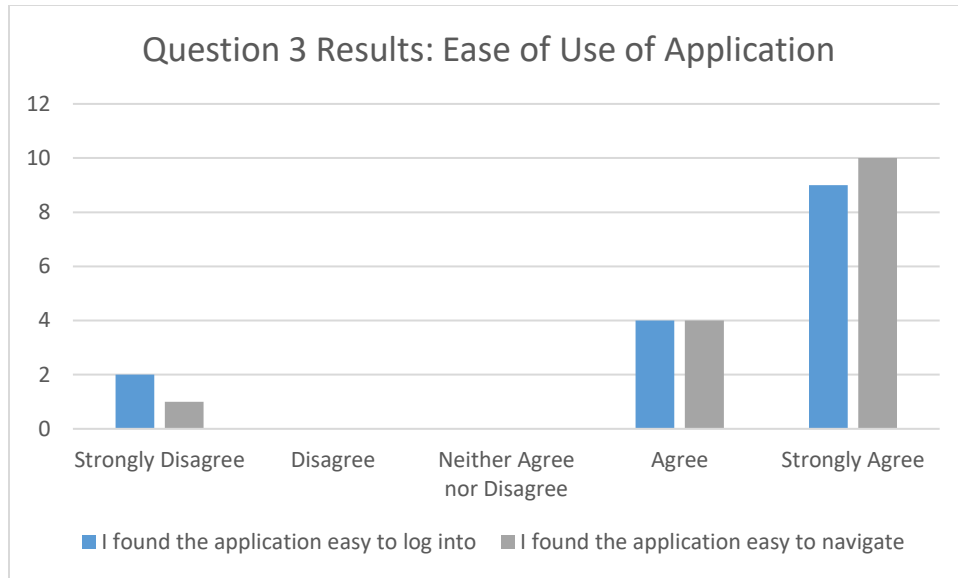


Figure F.a: Student Question 3 Results Bar Chart

F.1.4 Question 4

Question 4 asked participants about the usefulness of the learning materials throughout the application. It was a compulsory question. The results can be seen in Table F.d and Figure F.b.

Table F.d: Student Question 4 Results

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Average
I found the learning materials useful	0	1	0	3	11	15	4.6
I like the use of text-based resources	1	0	1	9	4	15	4
I like the use of video based resources	1	0	0	1	13	15	4.67

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Average
I like the use of image based resources	0	2	0	3	10	15	4.4
I like the use of audio based resources	0	1	0	5	9	15	4.47

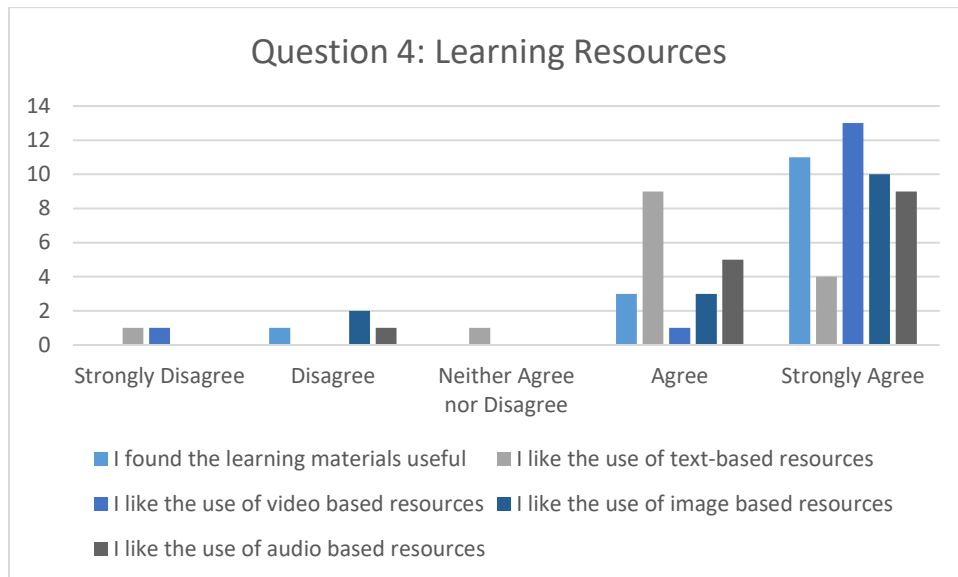


Figure F.b: Student Question 4 Results Bar Chart

F.1.5 Question 5

Question 5 asked respondents whether there were any additional features that they thought the application should have to help with the learning experience. There were six responses to this question in total. The results can be seen in Table F.e.

Table F.e: Student Question 5 Results

Is there any resources you would like to see more of?
No

Is there any resources you would like to see more of?
N/A
Interactive elements
Games
games
Games, a little more interaction would be nice

F.1.6 Question 6

Question 6 asked participants how useful they think the e-learning environment would be in teaching them cyber security and whether they think it would be used in schools. It was a compulsory question. The results can be seen in Table F.f and Figure F.c.

Table F.f: Student Question 6 Results

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Average
I think that using this system would help me to better understand cyber security	0	1	0	2	12	15	4.67
I can see my teacher asking us to use a resource like this	0	1	0	8	6	15	4

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Total	Average
By using this, I would learn more about cyber security than I would without it	0	1	0	3	11	15	4.6

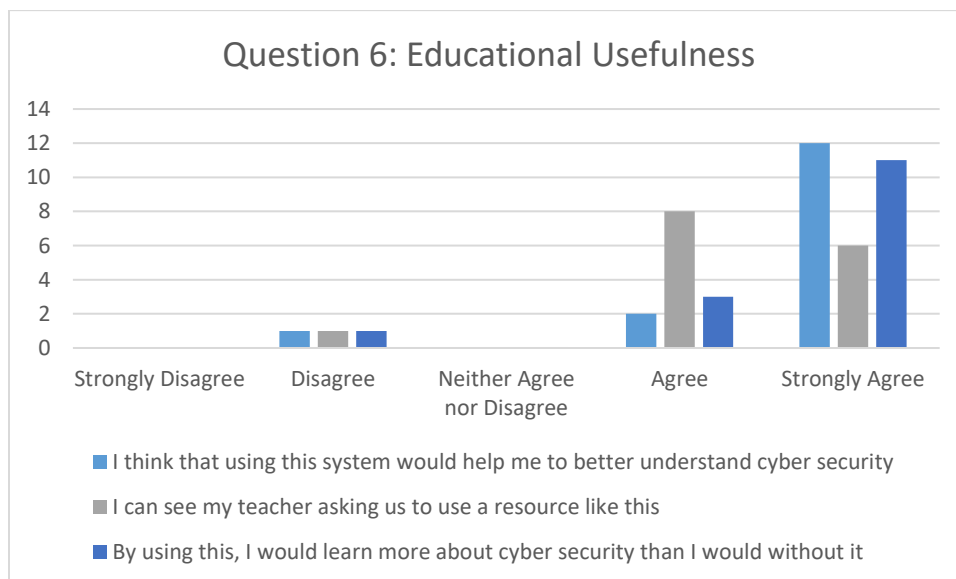


Figure F.c: Student Question 6 Results

F.1.7 Question 7

Question 7 asked participants if there are any additional features which should be added to the system. It was an optional question and received nine responses. The results can be seen in Table F.g.

Table F.g: Student Question 7 Results

What features would you like to be added to the system, and why?
More activities other than quiz questions

What features would you like to be added to the system, and why?
More quiz questions
N/A
Challenges that aren't exams or tests
Challenges other than quizzes and questioners
Challenges
Games to make learning more fun
games, more interactive
More games

F.1.8 Question 8

Question 8 asked if there were any features that respondents felt should be removed from the application. It was an optional question and received six responses. The results can be seen in Table F.h.

Table F.h: Student Question 8 Results

What features would you like to be removed from the system?
None
None
N/A
None
None
Nothing

F.1.9 Question 9

Question 9 asks respondents about any other improvements that can be made to the overall e-learning environment. It was an optional question and received 8 responses. The results can be seen in Table F.i.

Table F.i: Student Question 9 Results

Are there any other improvements that you think should be made to the solution?
No
Development for primary schools aswell as secondary!
N/A
None
More colourful
Bright Colours
Nicer looking website
No.

F.1.10 Question 10

Question 10 asks for any other general comments that respondants wish to make. It was optional and received seven responses. The results can be seen in Table F.j.

Table F.j: Student Question 10 Results

Any other comments
I found it easy to understand, everything was explained simply
Great idea!
No
No
Found it very easy to use, informative and engaging
No
I like the textboxes as there is not too much information but nice and short.

F.2 Student Quiz Results

Each student who took part in the evaluation had to take a quiz as part of the learning materials. The quiz questions and responses are provided in this section.

F.2.1 Questions

The respondents had four questions to answer in the quiz as part of the evaluation. Each respondent received the same four questions. The questions are detailed in Table F.k, with the correct answer to each question underlined.

Table F.k: Quiz Questions

	Answer 1	Answer 2	Answer 3	Answer 4
Question 1: Which of these could be considered a strong password?	Password123!	<u>0nR@!nyDa</u> <u>y5</u> <u>TheSun@!w</u> <u>ays</u> <u>C0mesOut</u>	abcdefgh	S3cure
Question 2: Which of these is not a factor in two-factor authentication?	Something you know	Something you have	<u>Something you think</u>	Something you are
Question 3: Which of the following pairs is an example of two-factor authentication?	password, date of birth	eye scan, fingerprint	usb stick, mobile phone	<u>password,</u> <u>fingerprint</u>
Question 4: Which of the following is not a type of network security device?	<u>Waterwall</u>	Intrusion Detection System	Firewall	Intrusion Prevention System

F.2.2 Question Scores

Respondants scores for each question are detailed in Table F.l, and participant's overall quiz grade is presented in .

Table F.l: Participant Scores

	Correct	Incorrect	Percentage Correct
Question 1	14	1	93%
Question 2	15	0	100%
Question 3	12	3	80%
Question 4	15	0	100%

Table F.m: Participant Quiz Scores

Participant ID	Quiz Score
10904	100
18007	100
32784	100
33461	100
33854	100
44553	100
51259	100
51269	75
62637	100
68321	75
74802	100
80192	75
87419	100
91836	100
99313	75
Average Score	93.33

F.3 Staff Evaluation Results

The results from each question in the staff evaluation are listed below.

F.3.1 Question 1

Question 1 asked participants for their participant ID. This was in order to identify responses should a participant ask to withdraw from the study. It was a compulsory question. The results can be seen in Table F.n.

Table F.n: Staff Question 1 Results

Please enter your participant ID	24630
----------------------------------	-------

F.3.2 Question 2

Question 2 asked participants to detail any issues that they had when using the application prior to the survey. It was an optional question. The teacher did not respond to question 2.

F.3.3 Question 3

Question three asked participants about how easy or difficult they found the application to use. It was a compulsory question. The results can be seen in Table F.o.

Table F.o: Staff Question 3 Results

I found the application easy to log into	Strongly Agree
I found the application easy to navigate	Strongly Agree

F.3.4 Question 4

Question 4 asked participants about the usefulness of the learning materials throughout the application. It was a compulsory question. The results can be seen in Table F.p.

Table F.p: Staff Question 4 Results

I think that the learning materials will help students in their understanding of the curriculum	Strongly Agree
I like the use of text-based resources	Strongly Agree
I like the use of video-based resources	Agree
I like the use of image-based resources	Agree
I like the use of audio-based resources	Agree

F.3.5 Question 5

Question 5 asked resonants whether there were any additional features that they thought the application should have to help with the learning experience. It was an optional question. The results can be seen in Table F.q.

Table F.q: Staff Question 5 Results

Is there any type of resource that you would like to see more of?	British English speakers
---	--------------------------

F.3.6 Question 6

Question 6 asked participants how useful they think the e-learning environment would be in delivering the cyber security security curriculum and whether they think it would be used in schools. It was a compulsory question. The results can be seen in Table F.r.

Table F.r: Staff Question 6 Results

I think that the system would help students to better understand cyber security	Agree
I can see this being used in schools	Strongly Agree
Teachers would find this resource useful in delivering the cyber security curriculums	Strongly Agree
Student would find this resource useful when learning about cyber security	Strongly Agree

F.3.7 Question 7

Question 7 asked participants if there are any additional features which should be added to the system. It was an optional question. The results can be seen in Table F.s.

Table F.s: Staff Question 7 Results

What features (if any) would you like to be added to the system, and why?	Interactive tasks to establish how secure a password might be. Research shows that "learning by doing" is effective.
---	--

F.3.8 Question 8

Question 8 asked if there were any features that respondants felt should be removed from the application. It was an optional question. The results can be seen in Table F.t.

Table F.t: Staff Question 8 Results

What features (if any) would you like to be removed to the system, and why?	The videos used lead directly to Youtube when they are finished. Is this intentional?
---	---

F.3.9 Question 9

Question 9 asks respondents about any other improvements that can be made to the overall e-learning environment. It was an optional question. The results can be seen in Table F.u.

Table F.u: Staff Question 9 Results

Are there any other improvements that you think should be made to the solution?	The colours on the sequence diagram made the text difficult to read for me. Lighter background colours might help.
---	--

F.3.10 Question 10

Question 10 asks for any other general comments that respondents wish to make. It was optional. The results can be seen in Table F.v.

Table F.v: Staff Question 10 Results

Do you have any other comments?	Penetration testing: some further explanation of terminology might be helpful for the youngest students.
---------------------------------	--

Appendix G: Design & Functionality

G.1 Conceptual Design

Images have been sketched to provide an overview of how the developed e-learning environment will look when finalised. The UI design will be finalised after the other High Priority development tasks have been completed, and as such may change before issuance of the final report. The key pages within the application are outlined below, along with images representing the planned interface design.

G.1.1 Login

All users authenticate through the same login screen. This allows users who have multiple roles (e.g. school administrator and teacher) to access all of their functions from one single login. An initial design of this page is shown in Figure G.a.

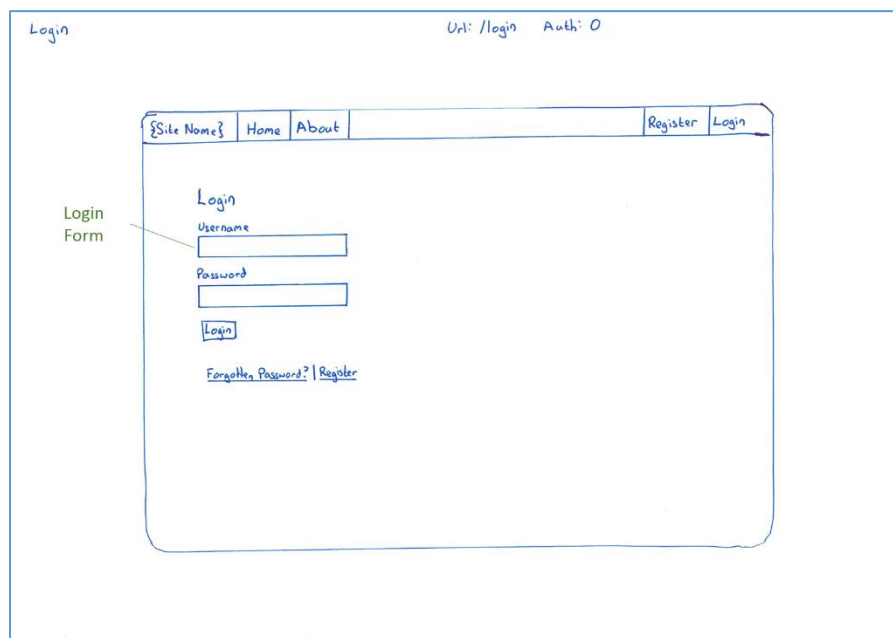


Figure G.a: Login Page

G.1.2 My Profile Page/Dashboard

Figure G.b shows the conceptual design for the profile page. The user profile page will be the default page that a student is shown when they log in. The page will show the student's current progress, with a link to continue with the next topic to the one previously completed. A link to a list of topics which students have flagged for revision is also prominently placed on the profile page. Statistics will also be shown to the user in order to bring an element of gamification to the system, as discussed by Barata *et al.* (2013).

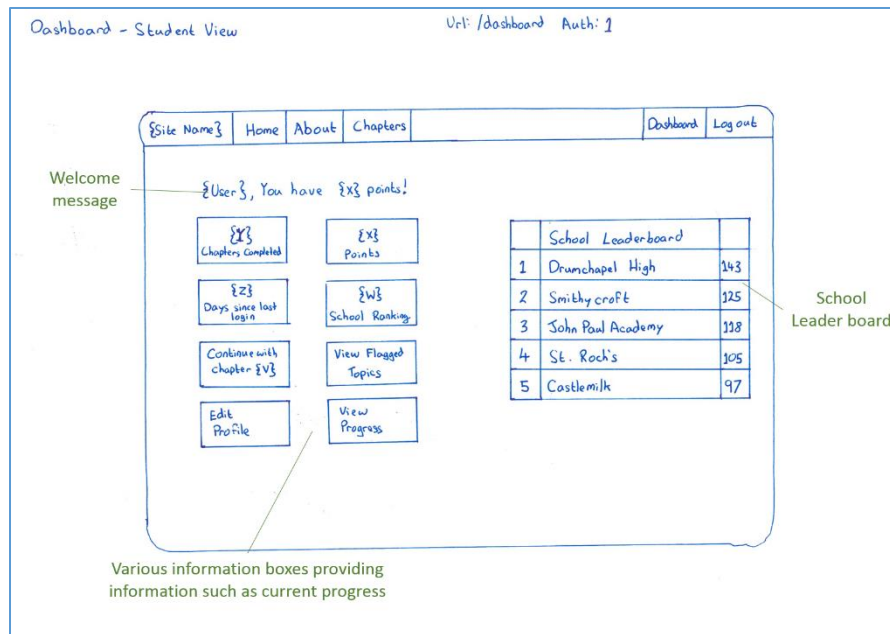


Figure G.b: User Profile Design Concept

Hunter (2016) proposed an inter-school leader board which will encourage participation as students will want to beat the other schools on the board. This leader board will be displayed on the right hand side of the profile page.

G.1.3 Chapter List

All of the chapters available to students is available on the Chapter List page, as shown in figure Figure G.c. This makes it easy for students to select which topic they want to study. A button enabling them to continue with where they left off is also provided.

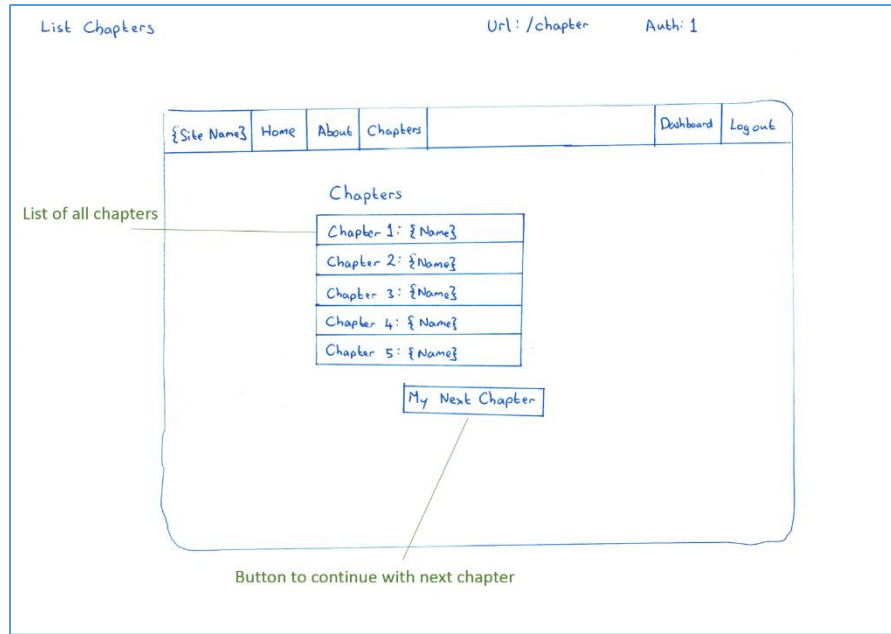


Figure G.c: Chapter List

G.1.4 Chapter Introduction & Topic List Page

Each major topic within the e-learning environment will have an introduction page outlining the major learning objectives within the chapter. There will be a navigation bar down the left hand side of the screen to allow users to navigate to specific topics within the chapter, as well as a button placed beneath the description to lead the user onto the first topic within the chapter. An image or introductory video will be displayed on the right hand side of some pages. The conceptual sketch for the Chapter Introduction page is shown in figure Figure G.d.

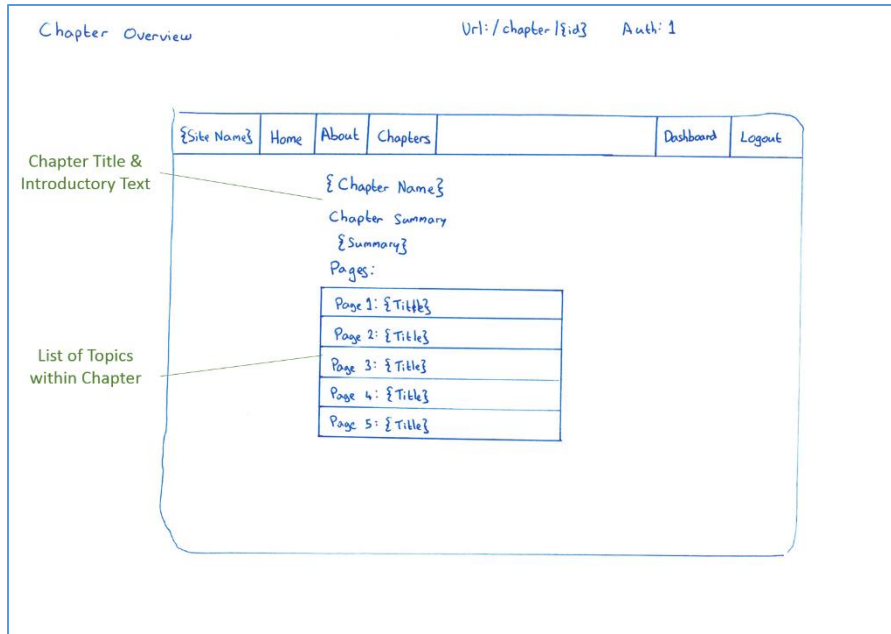


Figure G.d: Chapter Introduction & Topic List Design Concept

G.1.5 Topic Page

Each chapter consists of a number of topics. Each topic will be displayed on its own page within the e-learning system, and will consist of text for the user to read. Some topics will have videos or audio to help to explain the concepts within the topic. Each topic will also have buttons that the user can click to add the topic to a revision list or flag the question so that the teacher knows that the student needs more help with the topic. A conceptual design for the topic pages is shown in Figure G.e.

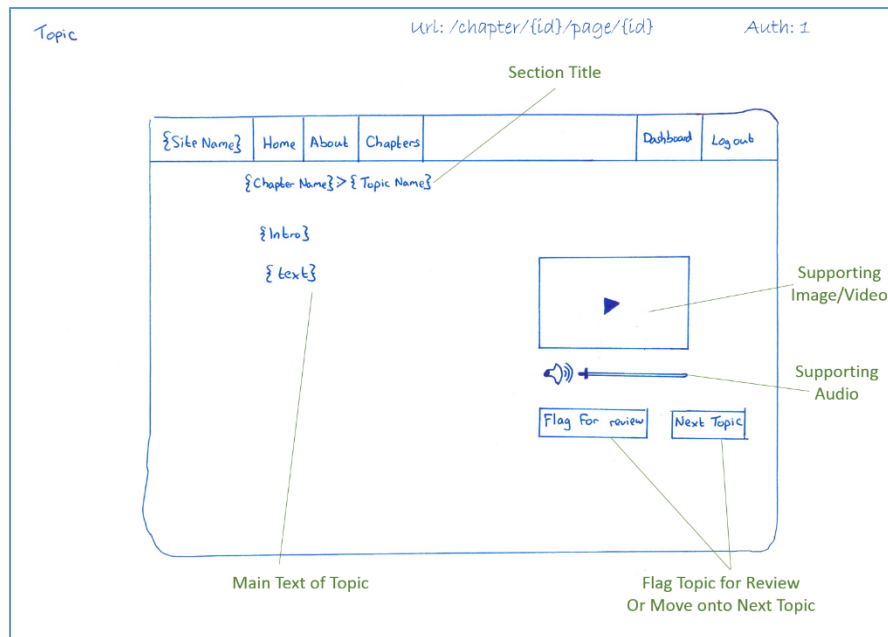


Figure G.e: Topic Within Chapter Design Concept

G.1.6 Quiz

Quizzes to test users' knowledge are also provided within each chapter. These can be used to help students in their studying, or assigned as examinations for students. A sample quiz is shown in Figure G.f.

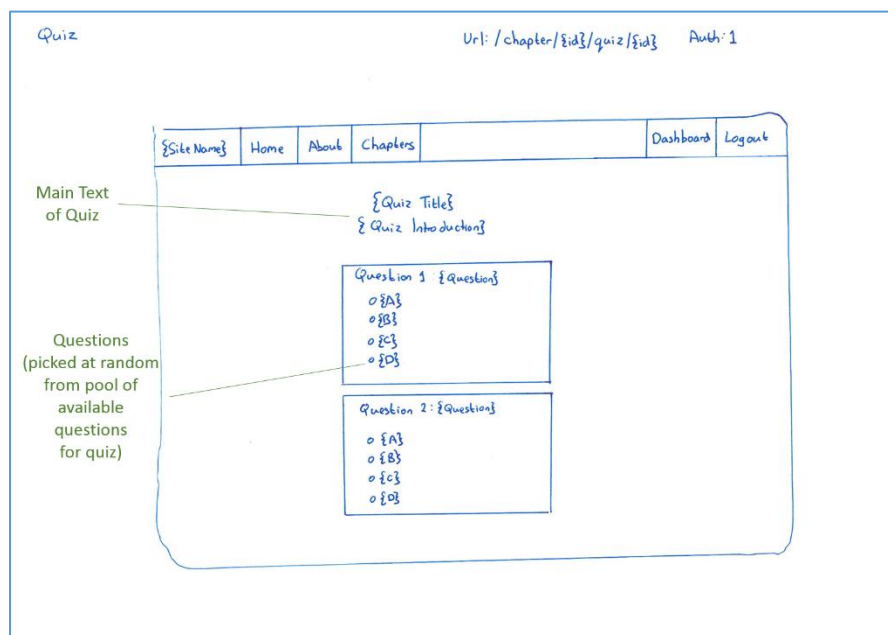


Figure G.f: Quiz Design Concept

G.1.7 Quiz Results

When a user completes a quiz, they can instantly view their grade, along with the answers they got correct and incorrect. A sample results page is illustrated in Figure G.g.

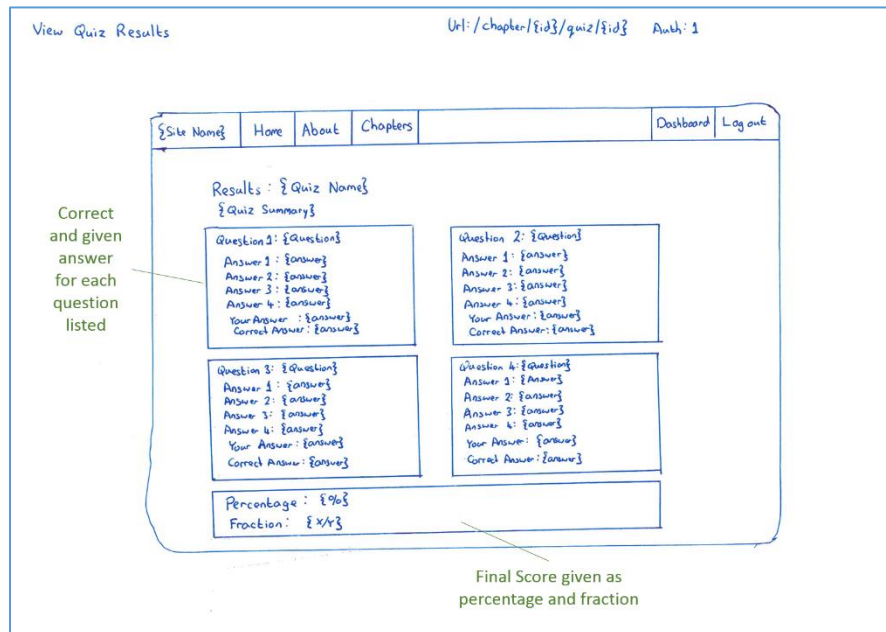


Figure G.g: Quiz Results Design Concept

G.1.8 View Classes

Teachers will have the ability to view each class that they teach. This will show the number of students that are in each class, as well as information about any messages or help requests sent by students to the teacher. A conceptual design for the “My Classes” page is shown in Figure G.h.

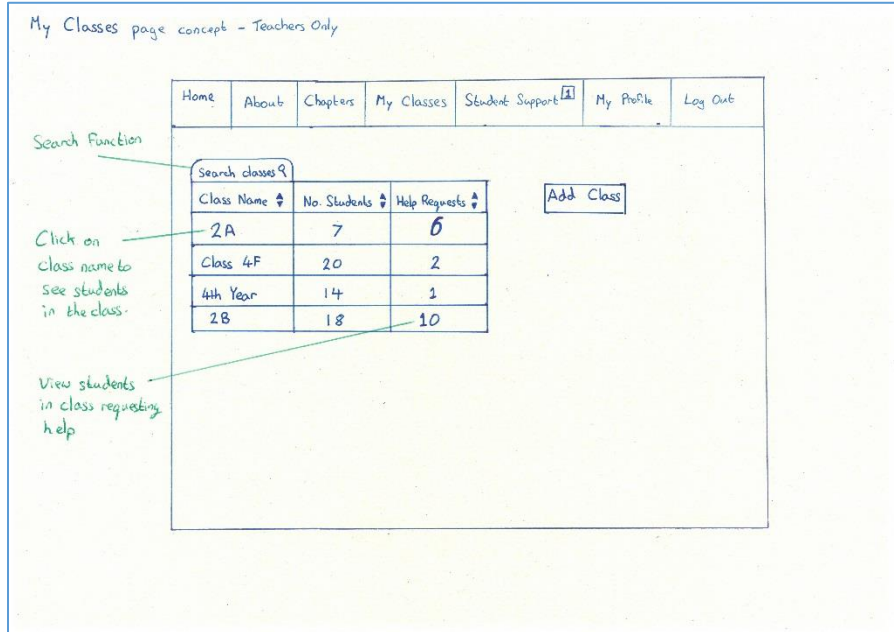


Figure G.h: My Classes View Design Concept

G.1.9 View Students

Teachers will be able to view information about each student in a class, including the topic that they last looked at, and any help requests or messages that they have submitted. The teacher will also be able to view detailed information about each individual student and their progress. A conceptual design for this page is shown in Figure G.i.

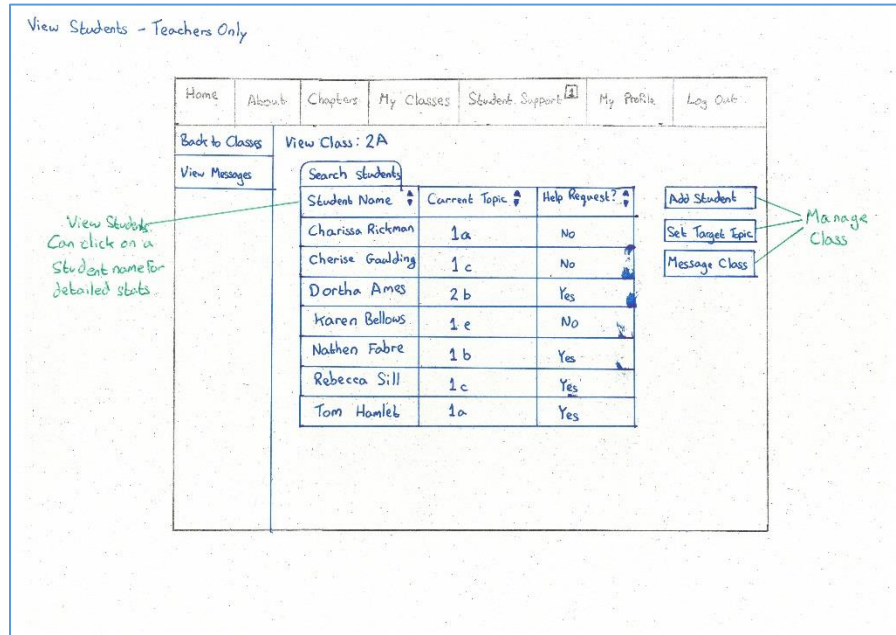


Figure G.i: View Students View Design Concept

G.1.10 Forgotten Password

If a user has forgotten their password for the application, there is an easy password reset process. The user enters their email address or username into the forgotten password box, and then receive an email with a reset link. Figure G.j shows this form.

Figure G.j: Forgotten Password Design Concept

G.1.11 Force Password Change

Once a user has successfully followed the forgotten password process, they are required to set a new password. The form to do so is shown in Figure G.k. If the user chooses to change their password from their profile, they will be asked to enter their current password in addition to the new one.

Figure G.k: Password Change Design Concept

G.2 Application Navigation

Analysis of existing e-learning platforms established that the UI is important in keeping users engaged. The application should be easy to navigate and use. The structure of the application from the three main user roles is outlined in Figure G.1 - Figure G.n.

Unauthenticated User

Users who have not logged into the application will have access to three pages: Home; About; and Login, as shown in Figure G.1. This will allow users to access their accounts whilst ensuring that they can only access authorised information.

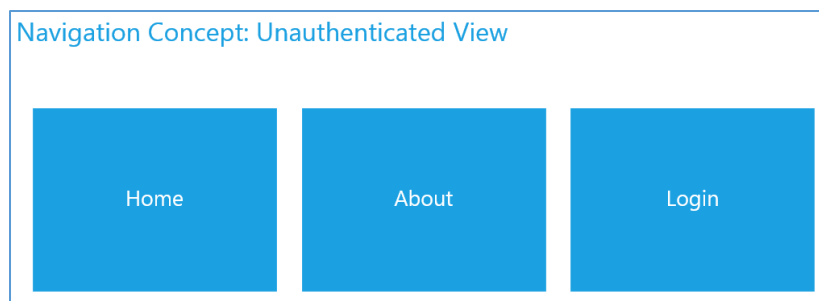


Figure G.1: Unauthenticated User Navigation

Student View

Authenticated Students within the application have the ability to view course content, and view /modify their profiles and progress. The pages available to authenticated students are outlined in Figure G.m.

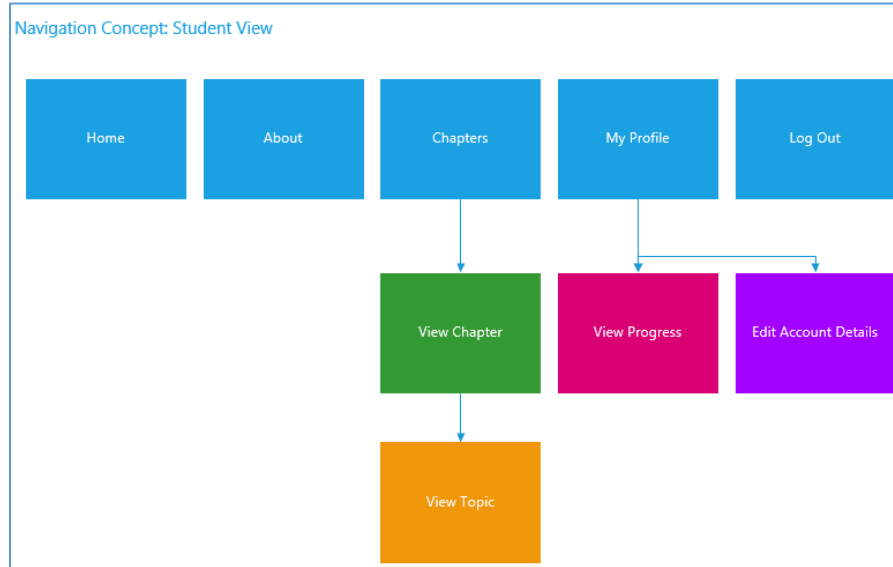


Figure G.m: Student's Navigation

Teacher View

Authenticated Teachers have the ability to view and manage their classes and students, as well as view and respond to student questions. This is in addition to the functionality that students can access. Teacher's navigation is outlined in Figure G.n.

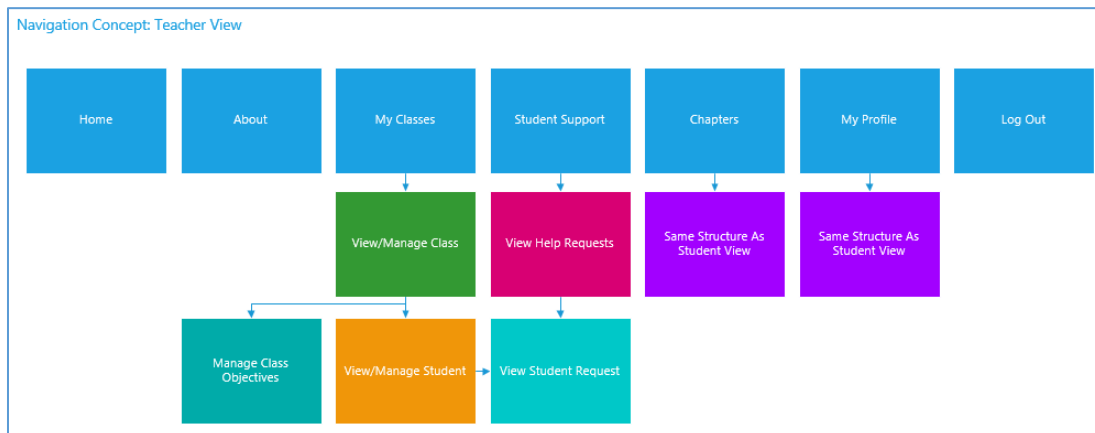


Figure G.n: Teacher's Navigation

G.3 Database Schema

The e-learning environment's database schema as devised in the initial project planning stage is provided on the following two pages (Figure G.o & Figure G.p) in the form of a Crow's Foot diagram. Note that the final database structure has changed significantly from these original design concepts, and are available in Appendix H: Project Architectural Design.

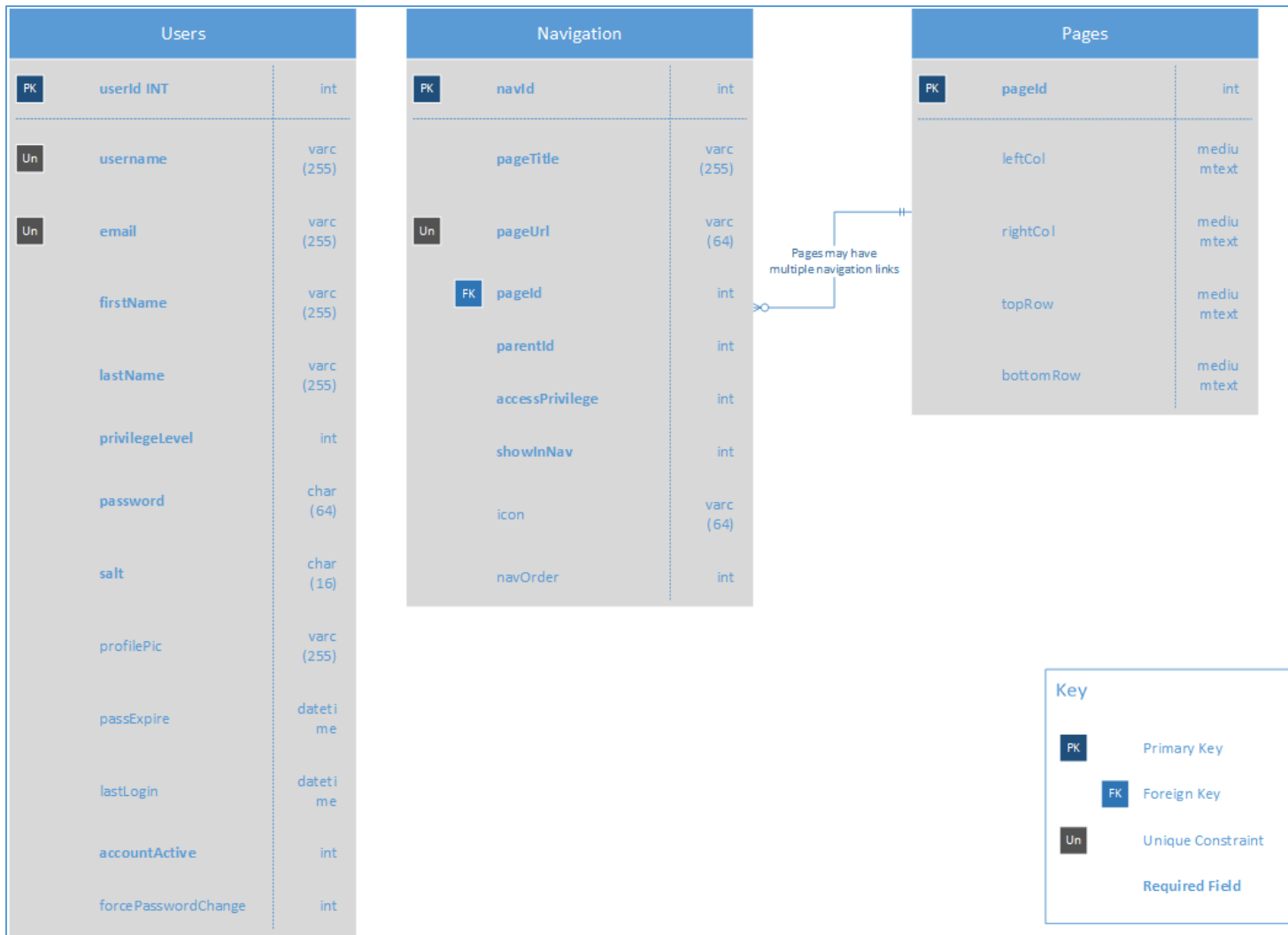


Figure G.o: Database Scheme Image 1

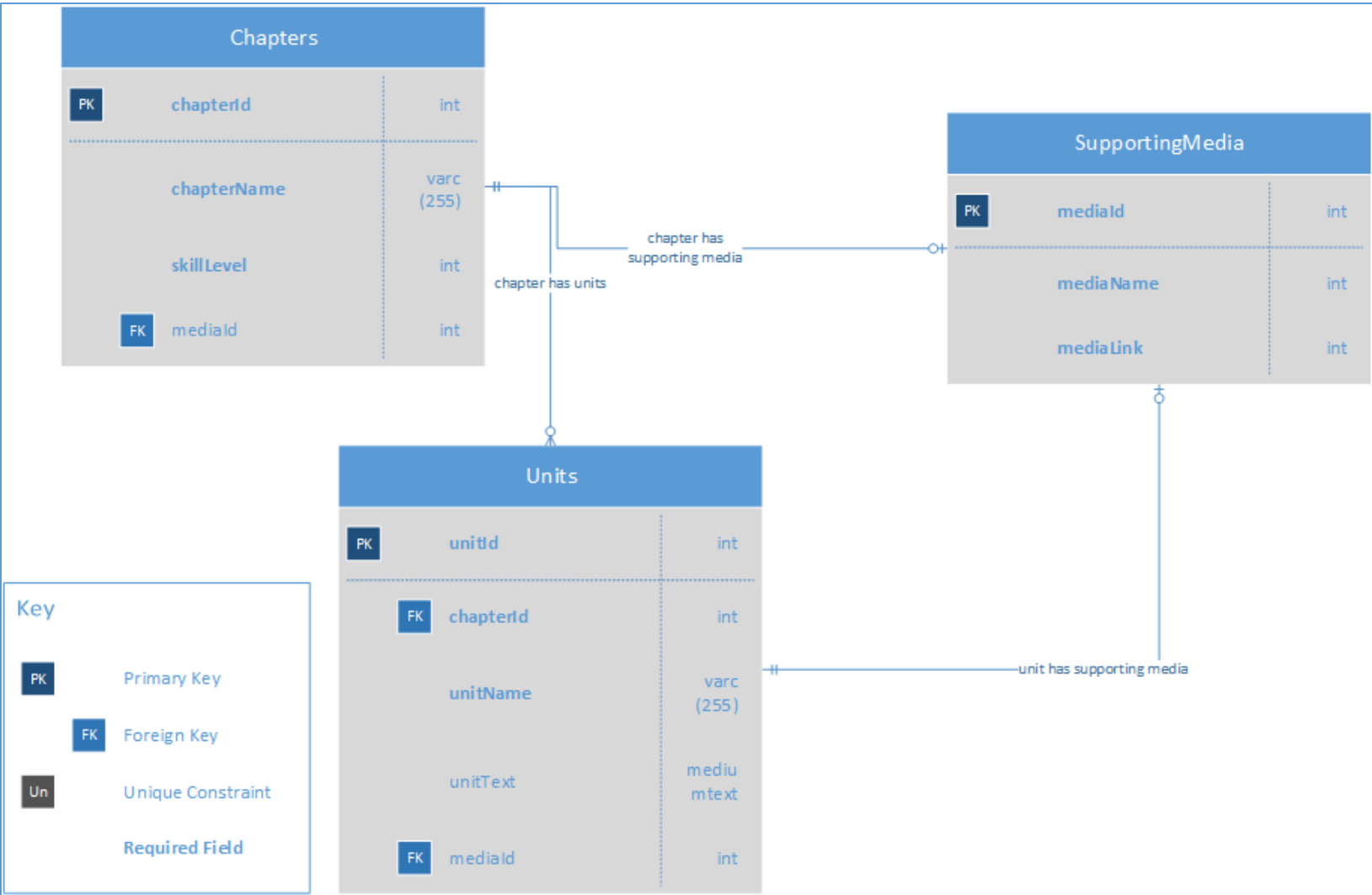


Figure G.p: Database Schema Image 2

Appendix H: Project Architectural Design

H.1 Navigational Structure

The final structure for each of the three main user roles (unauthenticated, student, teacher) is shown in Figure H.d, Figure H.b, Figure H.c.

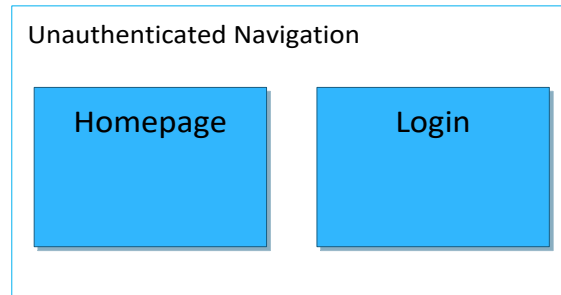


Figure H.a: Unauthenticated User Navigation

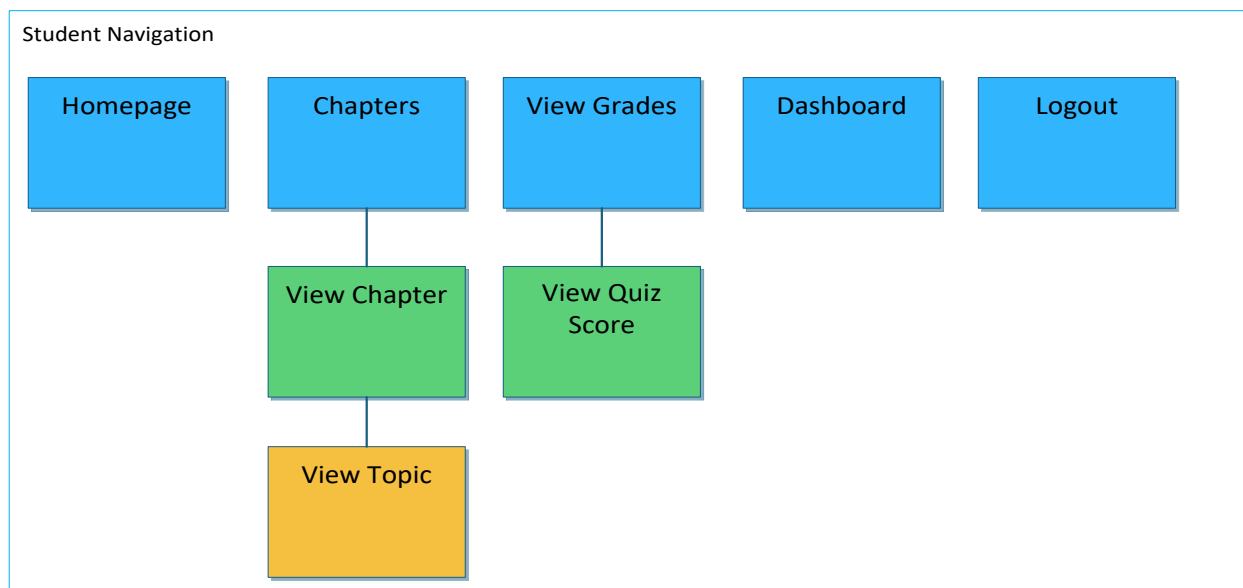


Figure H.b: Authenticated Student Navigation

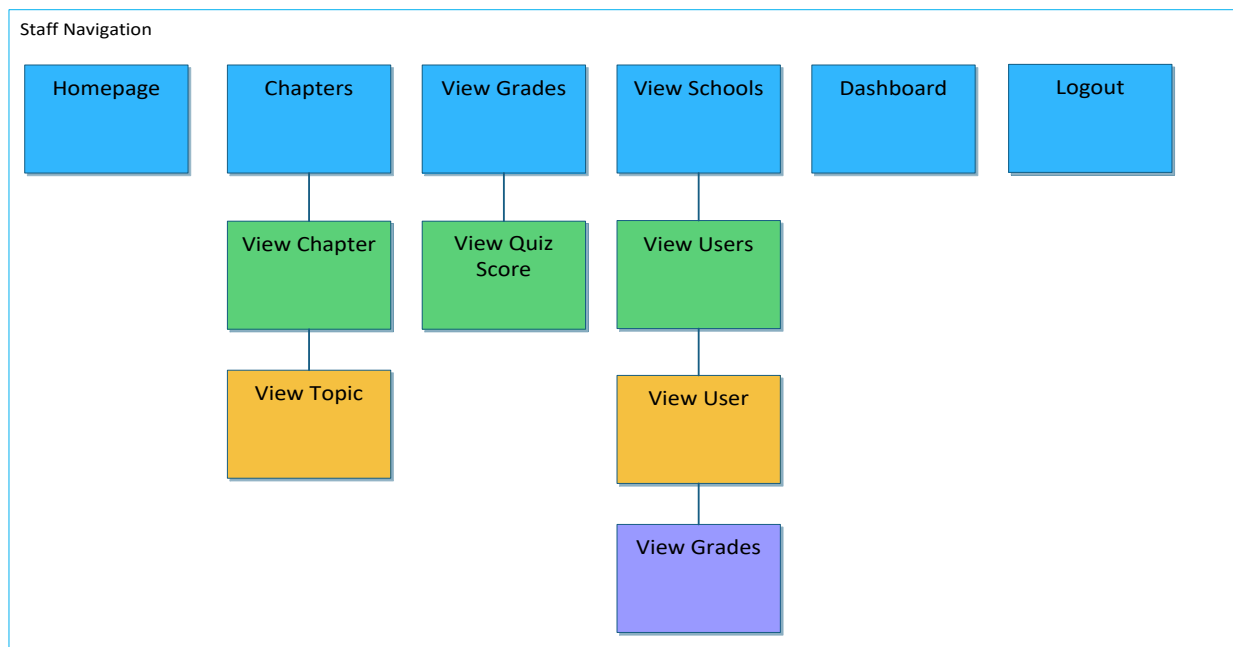


Figure H.c: Authenticated Teacher Navigation

H.2 Final Database Schema

The application's database schema uses the Crow's Foot database notation. Crow's Foot is a commonly used method of displaying database schemas in a clear manner, showing attributes including primary keys, foreign keys and relationship types (Cherwinka, 2012).

A key for the various symbols in Crow's Foot notation is shown in Table H.a, and the database schema is shown in Figure H.d: Final Database Schema.

Table H.a: Crow's Foot Notation Key

Notation	Meaning
	One and only one
	One or many
	Zero or one
	Either zero, one, or many

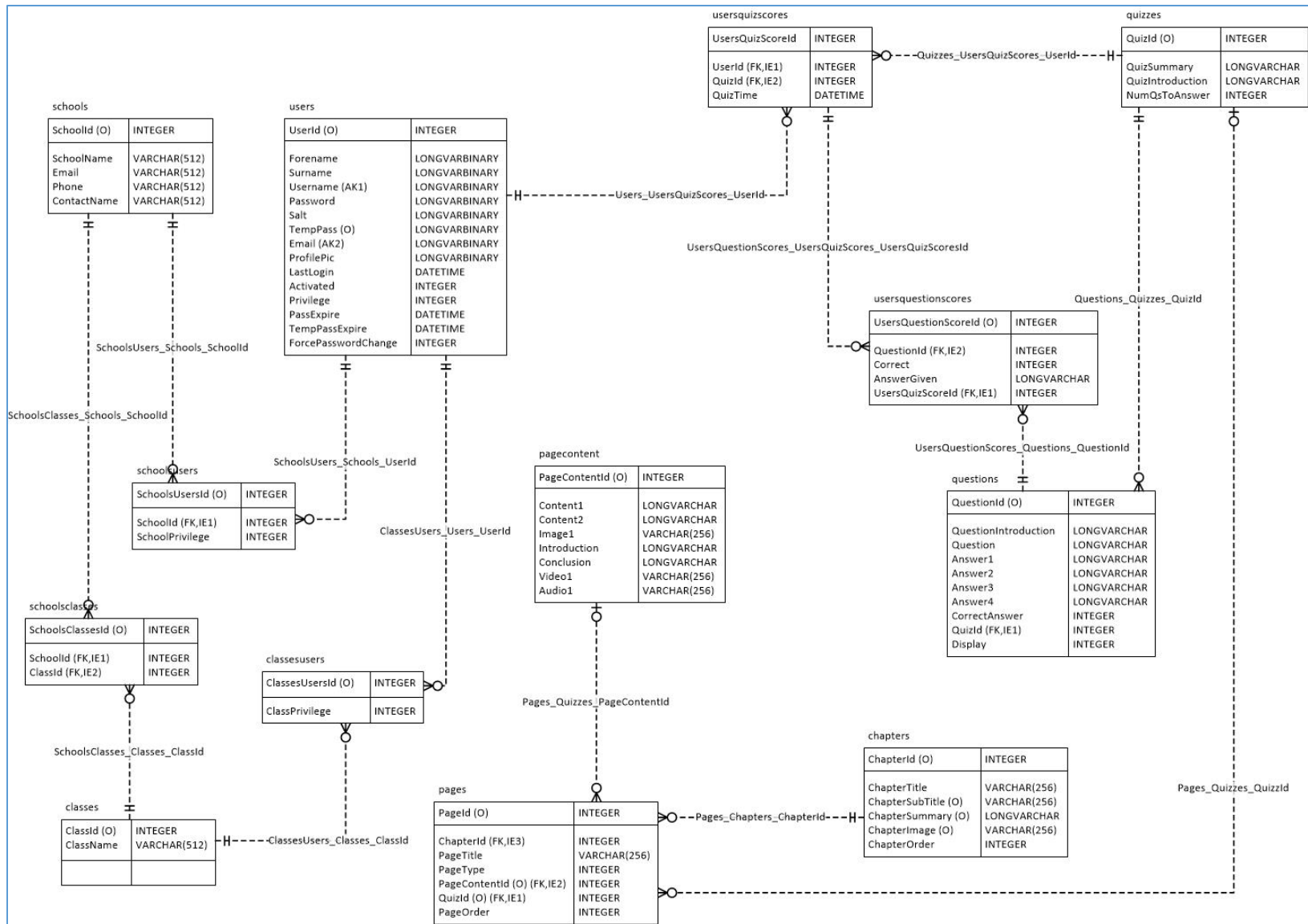


Figure H.d: Final Database Schema

Appendix I: Test Cases

Test Number	Test Description	Expected Result	Actual Result	Passed Test?
Unauthenticated Tests				
T1-Un	Login with correct credentials	User is authenticated to the application	As Expected	Yes
T2-Un	Login with incorrect username	Error message is displayed	As Expected	Yes
T3-Un	Login with incorrect password	Error message is displayed	As Expected	Yes
T4-Un	Entering username into forgotten password process	An email is sent to the user with a reset link	As Expected	Yes
T5-Un	Entering email address into forgotten password process	An email is sent to the user with a reset link	As Expected	Yes
T6-Un	Following active password reset link	Authenticates user and forces new password	As Expected	Yes
T7-Un	Following expired (time) password reset link	Error message displayed	As Expected	Yes
T8-Un	Following expired (used) password reset link	Error message displayed	As Expected	Yes
T9-Un	Following invalid password reset link	Error message displayed	As Expected	Yes
Authenticated Tests (Generic User)				
T10-Ag	Logout	Session is destroyed and user logged out	As Expected	Yes
T11-Ag	Navigate to Chapters page	A list of chapters is displayed	As Expected	Yes
T12-Ag	Navigate to a chapter	A list of pages within the chapter are displayed	As Expected	Yes

Test Number	Test Description	Expected Result	Actual Result	Passed Test?
T13-Ag	Navigate to a learning page	Learning content is displayed	As Expected	Yes
T14-Ag	Click “Previous Page” button within learning page	The previous learning page is displayed	As Expected	Yes
T15-Ag	Click “Next Page button within learning page	The next learning page is displayed	As Expected	Yes
T16-Ag	Navigate to learning page quiz	A quiz is displayed	As Expected	Yes
T17-Ag	Completing a quiz and submitting	A quiz results page is displayed showing which answers were correct and incorrect	As Expected	Yes
T18-Ag	Navigating to ‘View Grades’ Page	A summary of all quiz attempts by the user is displayed	As Expected	Yes
T19-Ag	Viewing a specific grade	A breakdown of which questions the user answered correctly and incorrectly is shown, as well as the grade.	As Expected	Yes
Authenticated Tests (Teacher)				
T20-At	Clicking View Users	Displayed the users’ school(s)	As Expected	Yes
T21-At	Clicking on a School	Displays the schools’ users	As Expected	Yes

Appendix J: Test Data

One hundred test user accounts were generated using data from generatedata.com (Keen, 2016). The test accounts are listed in Table J.a. Each test account was assigned to a school and class by the author.

Table J.a: Test User Data

Name	Surname	Username	Email	Active	Access	Pass Change	Password	LastLogin
Adele	Sweet	Adele.Sweet	feugiat@Morbinon.com	1	1	0	ZyL7iQI07bF3A4	2016-07-15 01:31:25
Alexandra	Dominguez	Alexandra.Dominguez	eu@ametluctusvulputate.ca	1	1	0	GNV0DhP37YB1h2	2016-02-08 11:04:38
Alika	Cleveland	Alika.Cleveland	Nunc.pulvinar@eutellusPhasellus.edu	0	1	0	LNu3LVT86qb2F7	2017-02-19 09:11:09
Avye	Mason	Avye.Mason	et.magnis.dis@insectetuer.net	1	1	0	IHt8awG53Sf7d5	2016-11-22 01:18:43
Beau	Wynn	Beau.Wynn	Proin.vel.nisl@mattis.co.uk	1	1	1	mVg4LdK81cj6s8	2016-07-08 16:22:45
Beck	Yates	Beck.Yates	turpis@arcuSed.net	1	1	0	lfP9OQt98wH7VE	2016-04-28 04:35:28
Benedict	Decker	Benedict.Decker	cursus.vestibulum.Mauris@pellentesqueSed.co.uk	1	1	1	zRY6ISO43IF9SD	2016-03-06 09:55:28
Bertha	Rocha	Bertha.Rocha	Cras.convallis@anunc.net	1	1	0	Ahp2MjW23Xe4JA	2016-09-08 07:58:06
Brandon	Miller	Brandon.Miller	ante@lobortis.org	1	1	0	pXy8tpS11Vv5G3	2016-06-22 12:09:19

Name	Surname	Username	Email	Active	Access	Pass Change	Password	LastLogin
Camille	Frye	Camille.Frye	gravida@odio.edu	1	1	0	XKt5qFh45Jb6GD	2016-10-11 09:30:52
Dacey	Mcbride	Dacey.Mcbride	eros.non.enim@lectuspedultrices.co.uk	1	1	0	LWu7rCP15UN118	2016-05-24 04:18:17
Danielle	Vincent	Danielle.Vincent	sit.amet.massa@feugiatSednec.edu	1	1	0	DwG7MQi11gc7z1	2016-10-06 16:12:32
Daquan	Briggs	Daquan.Briggs	lacus.Quisque.purus@sapien.net	1	1	1	cMg3GGC79KE5q5	2016-01-09 22:55:32
Daquan	Franks	Daquan.Franks	a@ategestasa.org	1	1	0	qKf9cHi22ax1r5	2016-03-22 18:58:19
Deirdre	Walters	Deirdre.Walters	malesuada.fringilla@doloregestas.edu	1	1	0	zL13iiE39ug9t8	2016-04-17 21:55:25
Desirae	Flores	Desirae.Flores	pretium.aliquet@Aeneanegestas.edu	1	1	0	rnj7UkO55Kj2j2	2016-10-03 05:11:53
Dieter	Sargent	Dieter.Sargent	Nulla.eget@Proinsedturpis.edu	1	1	0	VFg1rOY77mV3N1	2016-04-29 03:31:20
Echo	Ware	Echo.Ware	diam@vulputateullamcorper magna.edu	1	1	0	dUa4gcB37pM9FC	2016-01-04 13:03:01
Ella	Pruitt	Ella.Pruitt	a.sollicitudin.orci@nequeNullamnisl.edu	1	1	0	Qfp4xUD33kt2NE	2017-02-18 13:51:31
Ella	Key	Ella.Key	et.rutrum@arcuNuncmauris.co.uk	0	1	0	POh7Iye08Fx0QC	2017-02-10 02:28:10
Fitzgerald	Dominguez	Fitzgerald.Dominguez	Nulla.dignissim@Nunclectus.edu	1	1	0	mub6JKZ87Lp3I2	2016-01-01 17:41:29

Name	Surname	Username	Email	Active	Access	Pass Change	Password	LastLogin
Florence	Vazquez	Florence.Vazquez	amet.risus.Donec@quistriatique.co.uk	1	1	0	QYG9JMy38JC4GC	2017-02-08 17:30:14
Francesca	Stokes	Francesca.Stokes	in@Quisqueornare.com	1	1	1	emE7Yud69ey1v4	2017-01-04 07:05:23
Garrison	Oneill	Garrison.Oneill	adipiscing@auctorquistriatique.edu	1	1	0	FqU0jco28XL3U6	2016-02-06 22:13:44
Graiden	Frank	Graiden.Frank	mauris.ipsu@nostraperinceptos.edu	1	1	0	vKj4rcm22iA5S7	2016-09-11 03:00:51
Hakeem	Nunez	Hakeem.Nunez	Aliquam@nuncac.net	0	1	0	KMp7Gzr79oz2pE	2016-12-06 07:57:50
Halla	Pierce	Halla.Pierce	ac.arcu.Nunc@neccursusa.org	1	1	0	MGS7wNr06dC6lF	2017-01-16 15:06:13
Hammett	French	Hammett.French	tellus.eu.augue@fringillapurismauris.ca	1	1	0	WIE9ZLI97Uy2TE	2016-03-13 03:53:22
Hasad	Anthony	Hasad.Anthony	amet.risus.Donec@magnis.ca	1	1	0	gLn9QHe35Py2P8	2017-02-15 10:47:25
Heather	Hayden	Heather.Hayden	quis.turpis.vitae@sitamet.co.uk	1	1	0	fFI6xgw60Mx4F4	2017-03-10 16:21:20
Hedy	Cameron	Hedy.Cameron	cursus@accumsaninterdulibero.com	1	1	0	RRZ2Oty10SX6OA	2016-09-07 16:01:48
Herrod	Phillips	Herrod.Phillips	mus.Donec@erat.net	1	1	0	GFd7SiF59ge4V2	2017-02-26 00:22:21
Hope	Huff	Hope.Huff	ac.facilisis.facilisis@luctussit.ca	1	1	0	ZXP0aTt58id2v6	2016-07-30 15:30:57

Name	Surname	Username	Email	Active	Access	Pass Change	Password	LastLogin
Hoyt	Cotton	Hoyt.Cotton	lectus.convallis.est@semmolestie.net	0	1	0	pUR4pVo44px0dE	2016-01-23 21:44:42
Hyatt	Torres	Hyatt.Torres	erat.voluptat.Nulla@eu.co.uk	0	1	0	ilM0uif73dT0q2	2016-05-02 23:00:57
Idola	Hartman	Idola.Hartman	sit@ultricesDuis.org	1	1	0	xdA8JBC99ny0H8	2017-01-27 13:50:47
Ifeoma	Cameron	Ifeoma.Cameron	Curae@anteipsumprimis.ca	1	1	0	MUH1rhn01cB9c9	2016-08-13 06:12:08
Imelda	Jefferson	Imelda.Jefferson	rhoncus.id.mollis@necante.ca	1	1	0	gPE2NIv23mV9o3	2016-04-10 01:29:16
Indira	Simon	Indira.Simon	mollis.Phasellus.libero@acfacilisisfacilisis.edu	1	1	0	SfB7iwb30rr3VA	2016-03-19 10:43:52
Jack	Higgins	Jack.Higgins	Aliquam.fringilla@aliquetlobortisnisi.com	1	1	0	RYa2veq34MC6Y9	2016-11-10 09:26:13
John	Warren	John.Warren	diam.lorem.auctor@utsem.co.uk	1	1	1	TTM7UsS69rN3AF	2016-05-24 14:30:05
Jolie	Russo	Jolie.Russo	Morbi.quis@Phasellus.edu	1	1	0	UDU2zoR49Fb0Z9	2016-06-14 08:58:09
Jolie	Fitzgerald	Jolie.Fitzgerald	dolor@imperdietdictummagna.co.uk	1	1	0	zFs1MQh38Vf8J2	2016-04-11 20:32:11
Jordan	Alvarez	Jordan.Alvarez	parturient.montes@Nunccommodoauctor.net	1	1	0	Xdv1CUA47dS4hD	2016-03-01 13:35:22
Judah	McMahon	Judah.McMahon	aptent.taciti.sociosqu@convallisante.edu	1	1	0	uhk2EoF83tL1UD	2016-03-27 20:14:08

Name	Surname	Username	Email	Active	Access	Pass Change	Password	LastLogin
Kai	Hughes	Kai.Hughes	risus.at@maurisblanditmattis.ca	1	1	0	VBN3ZqC38rI1ED	2016-11-06 22:58:49
Kareem	Cooke	Kareem.Cooke	placerat@Nunclaoreetlectus.org	1	1	0	qbN2tgP86yq9V5	2017-02-28 21:22:50
Karly	Gentry	Karly.Gentry	risus@ridiculusmusProin.edu	1	1	0	kBW0sWg96eC5I2	2016-03-29 06:05:54
Katell	Clemons	Katell.Clemons	Aliquam.ultrices@massaMaurisvestibulum.org	1	1	0	CfB6vGC74UL0Z5	2016-11-09 13:54:58
Kenneth	Vasquez	Kenneth.Vasquez	risus.Donec@Loremipsumdolor.org	1	1	0	mQb6oxp03eE3mF	2016-07-21 05:05:37
Kerry	Reeves	Kerry.Reeves	lorem@Morbi.ca	1	1	0	dhz2dGF58bB2B0	2016-02-07 05:45:52
Kiyada	England	Kiyada.England	interdum.Sed@idmagnaet.ca	1	1	0	pFI9RWq55Mc2JA	2016-05-04 06:41:01
Lacota	Cantrell	Lacota.Cantrell	Nunc.ullamcorper.velit@mauriseu.com	0	1	0	XCf4LFY04oz7U4	2016-05-23 00:12:01
Lane	Harrell	Lane.Harrell	Fusce.mollis@nec.net	1	1	0	HDD2MBz53kC5q6	2016-07-02 01:13:38
Lareina	Compton	Lareina.Compton	cursus.luctus.ipsum@dolorFusce.org	0	1	0	rfG9taa56Sm6CD	2016-06-07 09:33:27
Lois	Baxter	Lois.Baxter	fames@neque.co.uk	1	1	0	YhP6OZZ21PR8QD	2016-01-06 15:23:57
Lunea	Bird	Lunea.Bird	lobortis.risus.In@nonegestas.com	1	1	0	QGV8ZRG76gI9TB	2016-08-04 02:39:49

Name	Surname	Username	Email	Active	Access	Pass Change	Password	LastLogin
Madaline	Mack	Madaline.Mack	tortor@tristiquealiquetPhasellus.co.uk	1	1	0	ueH8LnU76CV7kA	2016-04-29 04:59:24
Marvin	Valenzuela	Marvin.Valenzuela	varius.ultrices.mauris@elitfermentumrisus.net	1	1	0	ADp3wCS78st2ZA	2016-01-06 13:50:29
Meredith	Fuentes	Meredith.Fuentes	dignissim.tempor@velitQuisque.org	0	1	0	ifv0zkj22qq0n4	2016-05-28 20:57:24
Micah	Snyder	Micah.Snyder	interdum.enim@Nuncmauris.edu	0	1	0	WUi8cmS50px4QE	2016-03-20 10:39:47
Miriam	Williams	Miriam.Williams	a.felis@porttitorvulputateposuere.com	1	1	0	XsI0shL13aG7V6	2016-12-27 08:38:29
Montana	Irwin	Montana.Irwin	molestie.in@risus.edu	1	1	1	vyi5RFc67UG9W5	2017-03-08 05:59:15
Natalie	Vaughan	Natalie.Vaughan	Morbi.accumsan@Sed.com	1	1	1	gJR6DjU01zg9T8	2017-02-21 07:45:56
Neil	Gilbert	Neil.Gilbert	enim.Etiam@aliquam.net	1	1	0	qfY0RPw82CU5DC	2016-01-04 16:32:38
Nevada	Cobb	Nevada.Cobb	pellentesque.eget@maurisd.org	1	1	1	kWZ8Ngm97Dd6nB	2016-11-18 09:38:09
Neville	Martinez	Neville.Martinez	amet.risus@Nullam.org	1	1	0	mmU6HDc75HA7F7	2016-05-22 02:21:45
Nicholas	Palmer	Nicholas.Palmer	egestas.ligula.Nullam@duinectempus.edu	0	1	0	vsS5mdN74ny9t0	2016-12-25 17:12:30
Noelle	Saunders	Noelle.Saunders	est.Nunc@mienimcondimen	1	1	0	pNf1RwL04BG3bB	2016-12-11

Name	Surname	Username	Email	Active	Access	Pass Change	Password	LastLogin
			tum.co.uk					08:43:19
Octavius	Ayers	Octavius.Ayers	fringilla.porttitor.vulputate@NullamenimSed.org	1	1	0	YvJ8oRS50xL3r6	2016-05-19 11:38:38
Oliver	Howard	Oliver.Howard	id.blandit.at@netuset.co.uk	1	1	0	Vdn7rHW81oN1s6	2016-10-11 15:06:55
Otto	Shields	Otto.Shields	tellus.eu.augue@risusDonecnibh.net	1	1	0	utk4PJq94hK8A6	2016-03-24 20:10:33
Pamela	Larson	Pamela.Larson	Cum@quamPellentesque.edu	1	1	0	yVP5LyL30Ut8S5	2016-09-02 10:28:58
Priscilla	Hughes	Priscilla.Hughes	fermentum.arcu.Vestibulum@Duisrisus.org	1	1	0	vgB8fYM47Un5AE	2017-02-23 20:34:29
Quail	Bowman	Quail.Bowman	amet.diam@necmalesuada.ca	1	1	0	AqF9jzc90TI5EA	2016-06-16 18:10:49
Quintessa	Bryant	Quintessa.Bryant	Fusce@consectetuer.net	1	1	0	IcV6YAR34ko0sD	2016-05-21 16:33:05
Quynn	Walton	Quynn.Walton	dui.augue.eu@varius.edu	1	1	0	mSQ8Hah12TJ0d3	2017-02-04 09:48:38
Rajah	Mckenzie	Rajah.Mckenzie	dis.parturient@semper.net	1	1	0	INg0AEQ83eS7i1	2017-03-07 03:46:51
Rama	Morse	Rama.Morse	tincidunt@sapien.net	1	1	0	pIX4vNa23qS1S6	2016-05-17 10:46:56
Raphael	Waller	Raphael.Waller	nonummy.ut@convallis.com	1	1	0	Toc7gZR52Ad2m8	2016-02-11 09:02:52
Raphael	Decker	Raphael.Decker	Donec.nibh.Quisque@	1	1	0	FCv7jnD67fD4P9	2016-08-24

Name	Surname	Username	Email	Active	Access	Pass Change	Password	LastLogin
			libero.org					19:54:50
Roary	Ferrell	Roary.Ferrell	Nulla.interdum.Curabitur@miAliquam.edu	1	1	0	Mcj1CUi56zf1U2	2016-09-24 20:54:51
Robert	Snyder	Robert.Snyder	Curabitur.sed@Donecdignissimmagna.org	1	1	0	CED0UKN93gz4T9	2016-02-23 02:08:21
Rogan	Holloway	Rogan.Holloway	aliquet@nectempus.co.uk	1	1	0	oSF9HzQ61ju9WC	2016-03-20 16:42:00
Ronan	Bailey	Ronan.Bailey	neque@facilisisvitaeorci.co.uk	1	1	1	nvt9Kmb33zF0p3	2016-09-11 00:56:09
Rooney	Hays	Rooney.Hays	risus.a@lacuspedesagittis.ca	1	1	0	QxX6UGR80ZG1X6	2016-10-12 14:20:00
Rose	Navarro	Rose.Navarro	at.pretium@egestasSedpharetra.net	1	1	0	hvf7hZX45jr4i6	2016-10-04 05:21:28
Samantha	Burnett	Samantha.Burnett	neque.sed@erosturpisnon.edu	1	1	0	NkR4NaB83Qh1J5	2016-10-10 02:09:49
Sandra	Cannon	Sandra.Cannon	tristique.ac.eleifend@ipsumprimis.org	1	1	0	Mpt1kFW12HE5e2	2016-04-23 12:31:05
Sigourney	Osborne	Sigourney.Osborne	magna@fringillaornareplacerat.org	1	1	0	eSf4AXt81Zv0b7	2016-08-06 10:52:11
Skyler	Peterson	Skyler.Peterson	elit@ridiculusmus.edu	1	1	0	EYp2QuP27uK3f6	2017-03-09 12:25:57
Thaddeus	Vance	Thaddeus.Vance	Fusce.aliquet.magna@urna.net	1	1	0	kZf7hLk50Hb2kD	2016-07-01 12:51:11
Thomas	Hogan	Thomas.Hogan	lorem@placeratvelitQuisque	1	1	1	zdT6vCt60Fd0Y9	2016-05-09

Name	Surname	Username	Email	Active	Access	Pass Change	Password	LastLogin
			.ca					13:44:43
Vivian	Ballard	Vivian.Ballard	ut@leoVivamusnibh.net	1	1	0	Jdq4RjA79ig5P1	2017-01-27 03:09:45
Vivien	Pitts	Vivien.Pitts	vitae.aliquam.eros@dis.edu	1	1	0	RKR2Cdz73bQ6n8	2016-03-01 23:41:34
Wynter	Mclaughlin	Wynter.Mclaughlin	quis.diam.luctus@sapien.org	1	1	0	uUi1vHO97GJ7ZF	2016-10-27 09:14:49
Xavier	Myers	Xavier.Myers	libero@tempor.org	1	1	0	vMD2opz67dO0y9	2016-03-29 08:19:41
Xena	Mcmahon	Xena.Mcmahon	tortor.nibh.sit@utsemNulla.org	1	1	0	gve2MVT55uB3O1	2016-01-12 14:16:07
Zane	Williamson	Zane.Williamson	justo.faucibus.lectus@etnuncQuisque.ca	1	1	0	vlk6ShY81pv0gB	2016-03-31 19:30:16
Zenia	Ellis	Zenia.Ellis	tristique@Nullaeuneque.com	1	1	0	zSN7Imw65sf2x3	2016-09-29 18:13:40

Appendix K: Source Code

A lot of source code has been developed during the course of building the application. The code architecture has been discussed in Appendix H: Project Architectural Design. Source code has not been provided for publically available libraries which are available. Where this is the case, it has been documented in the relevant subsection and links to the online resource provided.

All of the code in the following subsections has been syntax highlighted by Beach's (2017) online syntax highlighter for word.

From this page until the end of the document (page CLXXX) has been redacted to avoid personal information or application source code disclosure. Contact the author if information from these page is required.