Programme of study for **Year 13 Information Technology**

Pearson BTEC Level 3 National Extended Certificate in Information Technology (AAQ) – Unit 2 (120 GLH, 2 hour 15 minute exam) and Unit 4 (60 GLH, coursework)

Autumn (1st term) Topic	Autumn (2nd term) Topic	Spring (1st term) Topic	Spring (2nd Term) Topic	Summer (1st term) Topic	Summer (2nd term) Topic
Unit 2: Cyber Security **A1 Cyber security threats** Internal and external threats; impact of a credible threat; the changing threat landscape (NCSC) **A2 System vulnerabilities** Vulnerabilities and sources of information; attack vectors; assessment tools; third-party review; penetration testing and OWASP; passive risk management	**Unit 2: Cyber Security** **A3 Legal responsibilities** GDPR; Computer Misuse Act 1990; areas of application **A4 Software and hardware security measures** Physical security; encryption; protecting a WLAN; secure design principles **Unit 4: Database – Task 1** **A1 Relational database management systems** RDBMS types; relational concepts; relational algebra; keys; integrity constraints; entity relationships **A2 Manipulating data** Defining, modifying and removing structures and data; queries and reports **A3 Normalisation** Anomalies; keys; UNF to 3NF **A4 Scoping a database solution** Purpose, research, technical vocabulary, logical structure	**Unit 2: Cyber Security** **B1 Network types** Network types; topologies; architecture; virtualisation **B2 Network components** Hardware components; external media and storage; software components **B3 Networking infrastructure services and resources** TCP/IP and TLS; domains and segmentation; network devices; DNS; file and print services **Unit 4: Database – Task 2** **B1 Design techniques and processes** Entity relationship modelling **B2 Design documentation** Data dictionary; user interface, queries and reports; automation; test and implementation plans; timescales **B3 Reviewing and refining designs** Self-review; refining; updating documentation	**Unit 2: Cyber Security** **C1 Cyber security documentation** Internal security policies and their effectiveness **D1 Forensic collection of evidence** Forensics on servers, PCs and mobile devices **D2 Systematic forensic analysis** Accurate records; assessing findings; writing security reports **Unit 4: Database – Task 3** **C1 Producing the database** Tables, relationships, validation, queries, reports, forms, automation, populating **C2 Testing** Test data; object and usability testing; feedback **C3 Reviewing** Quality, fitness for purpose, requirements **C4 Optimising** Data types and sizes; query efficiency	**Unit 2: Cyber Security** **Revision and exam preparation** Content areas A–D; command words; scenario and data-based questions; short- and long-answer technique **Unit 2 mock examination** 90 marks, 2 hours 15 minutes **Synoptic retrieval** Unit 1 networks, threats and legal issues linked to Unit 2	**Unit 2: Cyber Security** **External examination** May/June series (90 marks, 2 hours 15 minutes) **Unit 4: Database** **Resubmission window** Only if authorised by the Lead Internal Verifier

End of term 1 evidence to cover:		End of term 2 evidence to cover:		End of year evidence to cover:	
Unit 2: exam-style assessment on content areas A1–A4. Unit 4: Task 1 (learning aim A) completed.		Unit 2: exam-style assessment on content areas B, C and D, with retrieval of A. All Unit 2 content taught. Unit 4: Tasks 2 and 3 completed, so all Pearson Set Assignment Brief evidence (15 hours) is ready for internal marking and verification.		Unit 2: full mock, then the external examination (90 marks, 2 hours 15 minutes). Unit 4: internal verification complete.	
Rationale for sequence: Unit 4 does not start yet. Unit 2 is the larger unit, and content area A (threats and vulnerabilities) is the biggest section of the specification, so it gets undivided time first. Threats (A1) come before vulnerabilities (A2), so students know what they are defending against before learning how weaknesses are found and managed. Builds on Unit 1 content areas D and F from Year 12.	**Rationale for sequence:** Unit 4 coursework starts here. Task 1 is knowledge and scoping, and the relational concepts, SQL and normalisation it needs are new to students, so they are introduced early to give the longest run-up to the design and build tasks. Unit 2 finishes content area A with the legal responsibilities (A3) and the security measures that follow from the threats studied (A4).	**Rationale for sequence:** Unit 2 moves from threats to the networks being protected: types and topologies, components, then services such as DNS. This builds on Unit 1 content area B from Year 12, and gives the context needed for the policies and forensics that follow. Unit 4 Task 2 (design) follows the knowledge from Task 1, and designs are completed before any database is built.	**Rationale for sequence:** Policies (C) and forensic procedures (D) come last in Unit 2 because they are about responding to incidents, which makes more sense once threats, protection and networks are understood. Unit 4 Task 3 (build, test, review, optimise) comes last because it needs the designs from Task 2. Unit 4 finishes by the end of Spring 2 so Summer 1 is free for Unit 2 revision.	**Rationale for sequence:** All Unit 2 content has been taught before the assessment, as the specification requires. This half-term is for retrieval across areas A–D, exam technique on scenario and data-based questions, and a full mock to find gaps.	**Rationale for sequence:** Unit 2 is sat in the May/June series. Unit 4 resubmission, if authorised, takes place within 15 working days of results.
Home – Learning: Case studies of recent incidents: classify the threat and impact; NCSC threat report reading; vulnerability and attack vector retrieval cards.	Home – Learning: Unit 2: GDPR and Computer Misuse Act application questions; scenario question recommending security measures. Unit 4: practise SQL, keys and normalisation on non-assessed examples.	Home – Learning: Unit 2: network diagram and component identification tasks; DNS resolution explanation. Unit 4: wider reading on database design (non-assessed).	Home – Learning: Unit 2: forensic procedure sequencing; practise writing a security report from a scenario. Unit 4: wider reading on testing and optimisation (non-assessed).	Home – Learning: Past-paper style questions on weakest areas; revision plan built from the mock.	Home – Learning: Revision as directed.

Reading / High Quality Text: Specification: Unit 2, content area A. https://www.ncsc.gov.uk/ https://owasp.org/www-project-top-ten/	Reading / High Quality Text: Specification: Unit 2, content areas A3–A4; Unit 4, learning aim A. https://www.w3schools.com/sql/	Reading / High Quality Text: Specification: Unit 2, content area B; Unit 4, learning aim B.	Reading / High Quality Text: Specification: Unit 2, content areas C and D; Unit 4, learning aim C.	Reading / High Quality Text: Pearson sample assessment materials and past papers for Unit 2 (from the Pearson website).	Reading / High Quality Text: Specification: Unit 2 (all content areas).
Numeracy: Interpreting data on threats and incidents (percentages, trends).	Numeracy: Cardinality and counting records; interpreting query results.	Numeracy: Network addressing and ports; reading packet header data.	Numeracy: Data sizes and storage requirements (Unit 4 optimisation); hash values and checksums.	Numeracy: Exam practice: data interpretation and calculation questions.	Numeracy: Exam period.
Enrichment / opportunities to develop cultural capital (including careers, WRL and SMSC): Careers (nationalcareers.service.gov.uk job profiles): cyber security analyst, digital forensic analyst, database administrator, systems analyst. Progression: higher education IT, computing and cyber security courses (the progression route named in each unit). WRL: link database client briefs to real organisations or school needs. SMSC: data protection, privacy and the ethics of forensic investigation.					