THE ABBEY SCHOOL
A BUSINESS & ENTERPRISE ACADEMY

ICT AAQ L3

Scheme of Learning

Year 12+13

Mr Dannell

Topics by Term Year 12	Topic Overview for Year Group					
	Term 1	**Term 2**	**Term 3**	**Term 4**	**Term 5**	**Term 6**
Topics Taught	Unit 3 15 lessons - Learning Aim A: Understand how the principles of website development are used to create effective websites Unit 1 6 lessons	Unit 3 15 lessons - Learning Aim B: Explore website design skills and techniques to meet client requirements. Learning Aim C: Develop a website to	Unit 3 15 lessons - Coursework Unit 1 6 lessons - Learning Aim B: Transmitting data	Unit 1 15 lessons - Learning Aim D (Protecting data and information)/E (Impact of using IT systems) Unit 1 6 lessons - Learning Aim B:	Unit 1 15 lessons - Learning Aim D (Protecting data and information)/E (Impact of using IT systems) - Unit 1 6 lessons	Unit 1 15 lessons - Learning Aim F Issues Unit 1 6 lessons - Learning Aim C: Operating Online -

	- Learning Aim A: Explore the concepts and implications of the use of, and relationships among devices that form IT systems	meet client requirements Unit 1 6 lessons - Learning Aim A: Explore the concepts and implications of the use of, and relationships among devices that form IT systems -		Transmitting data -	- Learning Aim C: Operating Online	
Week Times	6 Weeks	7 Weeks	6 Weeks	6 Weeks	6 Weeks	7 Weeks

Topics by Term Year 13	**Topic Overview for Year Group**					
	Term 1	**Term 2**	**Term 3**	**Term 4**	**Term 5**	**Term 6**
Topics Taught	Unit 4 ???? lessons - Learning Aim A: Understand how the principles of relational database models, data storage and normalisation are used to create effective relational database solutions	Unit 4 ???? lessons - Learning Aim B: Design a relational database solution to meet client requirements - Learning Aim C: Develop a relational database solution to meet client requirements	Unit 4 ???? lessons - Coursework Unit 2 ????? lessons - Learning Aim C: Cyber security documentation	Unit 1 ???? lessons - Learning Aim D (Protecting data and information)/E (Impact of using IT systems) Unit 2 ???? lessons - Learning Aim D: Forensic procedures -	Unit 1 ??? lessons - Learning Aim D (Protecting data and information)/E (Impact of using IT systems) - Unit 2 ???? lessons - Exam Prep	

	Unit 2 ???? lessons - Learning Aim A: Cyber security threats, system vulnerabilities and security protection - methods	Unit 2 ????? lessons - Learning Aim B: - Use of networking architectures and principles for security				
Week Times						

Year 12 BTEC AAQ Information Technology Level 3

Unit 1: Information Technology Systems

Specification References	Topic Area: Main Items	Outcomes that students should be able to	Key Terms / Concepts (literacy)	Assessment	Resources
Unit 1 (LAA) Year 12 Term 1 and 2 **NWC 2 lessons a fortnight**	**A1: Functions and Use of Digital Devices, and Notation**	- Identify and describe a range of digital devices and their applications- Analyse technical features, benefits and limitations- Understand and apply flowchart and system diagram notations- Create and explain system diagrams and processes	- Digital devices (PCs, mobiles, embedded systems)- Flowcharts (symbols, logic)- System diagrams (components, connectivity)	- Group presentations- Paired case study reports- Flowchart creation task- Peer-taught system diagrams- **Know It All quizzes**- **Class test** on device types and notations	- PowerPoint slides- OneNote workbook- Textbook: *BTEC AAQ Student Book – Pearson*- Techopedia- Creately- Digital Divide Council- IDEA
	A2: Peripheral Devices and Media	- Identify and categorise input, output, and storage devices- Understand and evaluate assistive technologies- Compare characteristics of storage media- Explain manual vs automatic data processing	- Peripheral devices- Assistive tech- Storage media (capacity, cost)- Manual/automatic processing	- Student presentations- Written assistive tech reports- Comparison tables- Paired presentations- **Know It All quizzes**- **Class test** on peripheral/media types	- PowerPoint slides- OneNote workbook- Textbook: *BTEC AAQ Student Book – Pearson*- TechTerms- WebAIM- HowStuffWorks
	A3: Computer Software in an IT System	- Explain different operating systems- Compare types of user interfaces- Understand proprietary vs open-source software- Identify and convert file formats	- OS types- UI types (CLI, GUI)- Software licences- File types/formats	- Group research- Peer teaching- File conversions- Report on OS features- **Know It All quizzes**- **Class test** on OS/UI/software types	- PowerPoint slides- OneNote workbook- Textbook: *BTEC AAQ Student Book – Pearson*- Microsoft Learn- Codecademy- GCFGlobal- Quizlet
	A4: Choosing IT Systems	- Identify IT system types and match to user needs- Evaluate user requirements- Analyse effects of automation	- User needs- System compatibility- Performance- Automation in the workplace	- Class discussion- Case study research- Presentation on IT system choice- **Know It All quizzes**- **Class test** on system selection and factors	- PowerPoint slides- OneNote workbook- Textbook: *BTEC AAQ Student Book – Pearson*- CIO.com-

					Gartner- ComputerWeekly
	A5: Emerging Technologies	- Describe and evaluate emerging technologies- Analyse their impact on performance- Explore ethical implications- Design an implementation plan	- Emerging tech (AI, IoT, VR)- IT system performance- Ethics (privacy, data use)	- Group presentations- Reflective essay- Tech implementation project- Mock assessments- **Know It All quizzes**- **Class test** on emerging technologies and implications	- PowerPoint slides- OneNote workbook- Textbook: *BTEC AAQ Student Book – Pearson*- TechCrunch- MIT Tech Review- Pew Research- IBM Watson- Future of Privacy Forum
(LAB) **Year 12 Term 3 and 4** **NWC 2 lessons a fortnight**	**B1: Connectivity**	- Explain wired and wireless data transmission methods- Compare different connection types (Bluetooth, USB, Wi-Fi, Ethernet)- Evaluate how connection types impact system performance- Create and present a data transmission plan based on user/organisation needs	- Data transmission- Wired/Wireless- Bluetooth, USB, Wi-Fi, Ethernet- Speed, reliability, security	- Group connection comparison- Paired data plan presentations- Individual report on performance impact- **Know It All Ninja quizzes**- **Class tests** on connection types	- PowerPoint slides- OneNote workbook- Textbook: *BTEC AAQ Student Book – Pearson*- Cisco Networking Academy- Network World- CompTIA- IEEE Xplore- How-To Geek- Lifewire
	B2: Networks	- Identify and describe network types and topologies- Analyse the advantages/disadvantages of topologies (star, ring, bus)- Evaluate the impact of network features on performance	- Networks (PAN, LAN, WAN, VPN)- Topologies (star, ring, bus)- Connectivity- Downtime, security	- Group topology posters- Written report/presentation on network performance- Whole class discussion- **Know It All Ninja quizzes**- **Class tests** on network structures and performance	- PowerPoint slides- OneNote workbook- Textbook: *BTEC AAQ Student Book – Pearson*- Cisco Networking Academy- CompTIA- IEEE Xplore- How-To Geek- Lifewire

	B3: Issues Relating to Transmission of Data	- Explain data transmission protocols (SMTP, HTTP, HTTPS)- Describe how file types and compression affect transmission- Explore the role of codecs in multimedia delivery- Evaluate security and performance implications of transmission methods	- Protocols (SMTP, HTTP, HTTPS)- File types (image, video, audio)- Compression (lossy, lossless)- Codecs (H.264, MP3)- Bandwidth, latency	- Group protocol presentations- Individual file type report- Compression workshop & codec comparison- Mock assessments- **Know It All Ninja quizzes- Class tests** on transmission issues and performance	- PowerPoint slides- OneNote workbook- Textbook: *BTEC AAQ Student Book – Pearson*- Tuts+ (Envato)- Digital Trends- IEEE Xplore- How-To Geek- Lifewire
(LAC) **Year 12 Term 5/6** **NWC 2 lessons a fortnight**	**C1: Online Systems**	- Explain online IT system features including cloud computing models- Compare IaaS, SaaS, PaaS, public, private, and hybrid cloud models- Reflect on remote working technologies (VPNs, Remote Desktop)- Evaluate factors in choosing online systems- Discuss ethical and cultural implications of online systems	- Cloud computing (IaaS, SaaS, PaaS)- Public/Private/Hybrid Cloud- VPN, Remote Desktop- Security, scalability, accessibility- Cultural bias, ethical use	- Group presentations on cloud models- Reflective writing on remote work- Paired checklist and system evaluation- Whole class discussion on ethics & access- **Know It All Ninja quizzes- Class tests** on cloud & online systems	- PowerPoint slides- OneNote workbook- Textbook: *AAQ ICT Student Book*- IBM Cloud Learn Hub- AWS Cloud Computing Portal- Know It All Ninja
	C2: Online Communities	- Identify different online communities and platforms- Evaluate user experience in platforms- Assess privacy/security of chosen platforms- Discuss cost and productivity issues related to online tools	- Social media, blogs, forums- Accessibility, availability- Privacy, security, data risks- Subscription, integration, training costs	- Group research on community types- UX evaluation workshop- Paired report on platform security/privacy- Whole class cost/productivity discussion- Mock assessments- **Know It All Ninja quizzes- Class tests** on online communities	- PowerPoint slides- OneNote workbook- Textbook: *AAQ ICT Student Book*- Common Sense Media- Digital Citizen- Buffer Blog- Sprout Social- Podcast Insights- Know It All Ninja
(LAD) **Year 12 Term 4** **MK 5 lessons a fortnight**	**D1: Threats to Data, Information, and Systems**	- Identify and describe types of data threats (e.g., viruses, hacking, social engineering)- Evaluate the consequences of data breaches on individuals and organisations- Develop a security policy proposal- Participate in role play to understand social engineering- Understand impact of natural disasters on data	- Viruses, worms, trojans- Hacking, phishing, social engineering- Natural disasters- Data breaches- Security policy- Disaster recovery	- Group poster or digital presentation on threats- Case study analysis (e.g., Equifax)- Individual security policy proposal- Role play & debrief on social engineering- **Class test and Know It All Ninja quizzes**	- PowerPoint slides- OneNote workbook- Textbook: *AAQ ICT Student Book*- CISA (Cybersecurity Threats)- Kaspersky (Threat Types)- Verizon DBIR (Case Studies)- Privacy Rights Clearinghouse-

					Infosec Institute- The Hacker News- NCSC (UK Guidance)
	D2: Protecting Data	- Describe data protection techniques (file permissions, encryption, MFA, antivirus)- Compare different antivirus software and firewall solutions- Evaluate encryption methods in practical scenarios- Analyse data breach case studies and propose protection strategies- Understand legislation and data protection principles	- Encryption (at rest, in transit)- Antivirus software- Firewalls- Multi-factor authentication (MFA)- Data protection strategies- GDPR, Data Protection Act	- Group presentations on protection techniques- Class debate: Free vs paid antivirus- Paired encryption comparison charts- Case study analysis (e.g., Target breach)- Proposal for improved protection- **Mock assessments and interactive quizzes**	- PowerPoint slides- OneNote workbook- Textbook: *AAQ ICT Student Book*- Data Protection Commission (DPC)- IAPP – Privacy resources- Kaspersky – Antivirus & Firewalls
(LAE) **Year 12 Term 4/5** **MK 5 lessons a fortnight**	**E1: Online Services**	- Describe features of online retail platforms- Conduct a survey and analyse online shopping trends- Evaluate online education platforms- Understand how transactional data is used in marketing- Reflect on the ethical implications of targeted advertising	- Online retail (e.g., Amazon, eBay)- Personalised recommendations- Online education (e.g., Coursera, Khan Academy)- Collaborative tools (e.g., Google Docs)- Transactional data- Targeted marketing- Ethical use of data	- Group presentations on online retail surveys- Paired evaluations of learning platforms- Individual reflection on data and marketing ethics- **Mock assessments and Know It All Ninja quizzes**	- PowerPoint slides- OneNote workbook- Textbook: *AAQ ICT Student Book*- Statista – Online Retail- EdSurge – Online Learning- Coursera- Khan Academy- Google Scholar
	E2: Using and Manipulating Data	- Distinguish between primary and secondary data- Evaluate reliability and bias in data sources- Design effective data collection tools (e.g., surveys)- Understand verification and validation- Analyse consequences of inaccurate data- Evaluate user interfaces for data collection	- Primary vs secondary data- Bias, reliability, accuracy- Data collection methods- Validation & verification- User interfaces- Data quality and decision-making	- Group research on data sources- Individual data collection tool design- Case study analysis on data accuracy- Paired evaluation of survey tools- Class debate on data reliability- **Mock assessments and interactive quizzes**	- PowerPoint slides- OneNote workbook- Textbook: *AAQ ICT Student Book*- Data.gov- Statista- SurveyMonkey- TDWI (Data Accuracy & Management)

(LAF) **Year 12 Term 6** **MK 5 lessons a fortnight**	**F1: Moral and Ethical Issues**	- Understand moral and ethical issues related to IT use- Explore topics such as privacy, environmental impact, and netiquette- Debate the use of technology in relation to privacy- Research and report on IT's environmental impact- Role-play scenarios to demonstrate positive and negative online behaviour	- Privacy & surveillance- User consent- Environmental impact- E-waste, energy use- Unequal access- Assistive technology- Online behaviour & netiquette- Acceptable use policies (AUPs)	- Group debates on privacy- Individual research report on IT and the environment- Paired netiquette role-play scenarios- Whole class discussions- **Mock assessments and quizzes**	- PowerPoint slides- OneNote workbook- Textbook: *AAQ ICT Student Book*- Electronic Frontier Foundation (EFF)- Privacy International- World Economic Forum- Environmental Protection Agency (EPA)
	F2: Legal Issues	- Understand key legal issues related to IT- Examine legislation like Computer Misuse Act, Copyright Law, GDPR- Analyse real-world misuse case studies- Explore health and safety regulations for IT use- Evaluate the impact of legislation on individuals and organisations	- Computer Misuse Act (1990)- Copyright law- GDPR / Data Protection Act- Health & safety (DSE regulations)- Ergonomics- Cybercrime- Legal implications for IT use	- Small group presentations on computer misuse cases- Individual infographic/report on copyright law- Ergonomics checklist activity- Class discussions on legal protection and data use- **Mock assessments and Know It All Ninja quizzes**	- PowerPoint slides- OneNote workbook- Textbook: *AAQ ICT Student Book*- UK Gov – Data Protection- Copyright.gov- Health and Safety Executive (HSE)- Information Commissioner's Office (ICO)- EU GDPR site- Cybercrime.gov

Unit 3: Website Development (COURSEWORK)

Specification References	Topic Area: Main Items	Outcomes that students should be able to	Key Terms / Concepts (literacy)	Assessment	Resources
LAA **Year 12 Term 1**	**A1: Purpose and Principles of Websites**	- Understand different purposes of websites: e-commerce, information, promotion, entertainment- Analyse how websites meet different user needs and purposes- Understand user demographics and typical user personas- Explore and identify the principles of good website design	- Website purpose- User demographics: age, gender, location, income, education- Layout, navigation, UX (user experience)- Consistency, SEO,	- Class discussion on website purposes- Independent research on website demographics- Website review task identifying key principles of design	- PowerPoint slides- OneNote workbook- Textbook: *AAQ ICT Student Book*- Amazon – e-commerce- Wikipedia – information- BBC iPlayer & Netflix –

			dynamic content- Accessibility and browser compatibility		entertainment- Apple – promotion
	A2: Planning a Website in Response to a Client Brief	- Understand how to read and interpret a client brief- Identify goals, problems, and target audience- Use questioning techniques to draw out client needs- Understand legal and ethical issues (copyright, data protection, accessibility)- Evaluate case studies on copyright and ethical content use	- Client brief- Website goals- Audience needs- Technical constraints- Copyright- Data protection- Digital accessibility- Case study analysis	- Whole class discussion on client briefs- Group consultation role-play activity- Case study analysis of copyright issues- Group task: key message extraction from a brief	- PowerPoint slides- OneNote workbook- Sample client briefs (e.g. GreenLeaf Organic Foods, GlowFit Gym)- Case study packs- Video clips on copyright & GDPR- UK Gov data protection site- Creative Commons
LAB **Year 12 Term 2** **MK 5 lessons a fortnight**	**B1: Website Design**	- Create and understand wireframes and visual designs for websites- Apply design principles such as layout hierarchy, alignment, balance, and dimensions- Understand visual styles: branding, colour palette, and typography- Evaluate how designs meet client needs and user requirements	- Wireframes- Visual styles- Layout hierarchy- Branding- Typography- Fitness for purpose- Client requirements	- Group wireframing task using model scenarios- Paired activity reviewing website designs- Evaluation of sample websites for fitness for purpose and clarity	- PowerPoint slides- OneNote workbook- Wireframe.cc – free wireframing tool- Sample client briefs- Examples of effective website designs
	B2: Asset Management Techniques	- Create and manage assets for use on websites (copy, images, icons, video)- Optimise and compress assets without losing quality- Understand copyright and royalty-free content usage- Organise assets with logical folder/file naming structures	- Copywriting- Image compression- Video trimming- Asset folders- File naming conventions- Royalty-free content- Image optimisation	- Paired image editing activity- Group asset scavenger hunt- Individual tasks: copywriting, image/video compression, logical folder structure	- PowerPoint slides- OneNote workbook- Unsplash, Pexels, Pixabay – royalty-free image/video sources- Flaticon, Font Awesome – icons- TinyJPG, Adobe Express – image compression- Handbrake – video compression
LAC	**C1: Common tools and**	- Write webpages using HTML- Enhance websites using CSS for layout, colours,	- HTML- CSS- JavaScript-	- HTML webpage task with embedded elements- CSS	- W3Schools HTML: https://www.w3schools

Year 12 Term 2 **MK 5 lessons a fortnight**	**techniques to produce a website**	typography, and responsive design- Apply JavaScript for interactivity (e.g. slideshows, animations, filtering content)- Understand integration of multimedia elements (video/audio)- Recognise role of SEO and visit a real-world web company if possible	Navigation (internal/external links)- Media elements (video, audio, forms)- SEO (Search Engine Optimisation)- Responsive design	styling and layout activity- JavaScript tutorial projects- Evaluation of site interactivity- Reflective summary from web company visit	.com/html/- W3Schools CSS: https://www.w3schools.com/html/html_css.asp - W3Schools JavaScript: https://www.w3schools.com/html/html_scripts.asp- W3Schools HTML video: https://www.w3schools.com/html/html5_video.asp- W3Schools HTML audio: https://www.w3schools.com/html/html5_audio.asp
	C2: Website development processes	- Evaluate websites for accessibility, client needs, legal and ethical issues- Apply WCAG (Web Content Accessibility Guidelines) and W3C HTML5 standards- Review and improve websites for target audience and consistency- Learn about website publishing steps (e.g. hosting, domains, pre-launch checks)- Create a publishing checklist	- Accessibility (alt tags, zoom, screen readers)- WCAG / W3C Standards- Legal & Ethical (copyright, data protection)- Website publishing- Hosting/domain setup- Design consistency- Target audience	- Individual website review task- Peer review session- Group discussion on publishing- Website checklist activity	- W3Schools Alt Tags: https://www.w3schools.com/tags/att_img_alt.asp- W3Schools Zoom: https://www.w3schools.com/accessibility/accessibility_page_zoom.php - W3C Validator: https://validator.w3.org - Reading Uni Website Evaluation: https://libguides.reading.ac.uk/evaluating-websites- BITLAW legal issues: https://www.bitlaw.com/internet/webpage.html- WebFX Readability Tool: https://www.webfx.co

					m/tools/read-able/- Webflow Publishing Guide: https://webflow.com/blog/how-to-publish-a-website
	C3: Testing	- Create and carry out website test plans- Test areas such as navigation, links, layout, and interactivity- Capture evidence of testing through screenshots and screen recordings- Conduct usability audits considering navigation, user experience, and accessibility	- Test plan- Functionality testing- Usability testing- Screen responsiveness- User experience (UX)- Accessibility	- Learner-created test plan- Test evidence log (screenshots/recordings)- Paired usability audit and peer feedback	- BrowserStack QA Testing Guide: https://www.browserstack.com/guide/how-to-perform-website-qa-testing
Course Work **Term 3** **MK 5 lessons a fortnight**	**Course Work**	Pupils using knowledge from previous learning pupils will need to complete the set brief. Hand in date END OF TERM 3			

YEAR 13 (PLAN TO BE DECIDED NEXT YEAR)

Unit 2 Cyber Security and Incident Management

Specification References	Topic Area: Main Items	Outcomes that students should be able to	Key Terms / Concepts (literacy)	Assessment	Resources
LA (1)	**A1.1.1: Employee sabotage (deliberate and accidental)**	- Differentiate between internal and external threats- Analyse scenarios involving sabotage or accidental data breaches- Understand risks of unauthorised software- Evaluate legal consequences of unsafe software use	- Internal threat- Sabotage- Accidental damage- Unauthorised software- Legal liability- Data breach	- Group scenario analysis presentations- Paired research & presentation on real-world legal cases -Know It All Ninja -Class Assessments	-OneNote and Class Presentation - NCSC Insider Threats: https://www.ncsc.gov.uk/- Get Safe Online: https://www.getsafeonline.org/- TalkTalk case: https://ico.org.uk/.../talk

					talk-cyber-attack...- FAST UK: https://fast.org/
	A1.1.2: Accidental or deliberate damage	- Recognise types of physical damage (fires, floods, power loss, terrorism)- Analyse risk and impact scenarios- Understand and evaluate disaster recovery strategies	- Deliberate damage- Accidental damage- Disaster recovery- Offsite backup- Redundancy systems	- Group analysis of real-life scenarios- Paired research on disaster recovery strategies	-OneNote and Class Presentation - NCSC Small Business Guide: https://www.ncsc.gov.uk/collection/small-business-guide- ICO Breach Reports: https://ico.org.uk/for-organisations/report-a-breach/...
	A1.1.3: Weak cyber security measures and unsafe practices	- Identify unsafe practices in workplace scenarios- Evaluate weak vs strong security measures- Propose improvements to reduce risk	- Unsafe practice- Cyber hygiene- Visitor access- Unsecure websites- Equipment security	- Group scenario activity- Paired research and presentation on security measures -Know It All Ninja -Class Assessments	-OneNote and Class Presentation - UK Government Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework
	A1.1.4: Accidental loss or disclosure of data/credentials	- Understand causes of accidental data loss- Analyse consequences of human error- Assess how human factors affect data security- Propose preventative measures	- Human error- Data disclosure- Security culture- Training- Monitoring	- Group case study analysis- Pair presentations on human factors and solutions -Know It All Ninja -Class Assessments	-OneNote and Class Presentation - Public Health Wales case: https://www.itgovernance.co.uk/blog/public-health-wales-accidentally-publishes-18000-coronavirus-patients-data
	A1.2.1: Malicious software (malware)	- Identify different types of malware- Match symptoms and characteristics of each type- Research and explain current prevention methods	- Malware- Virus- Worm- Trojan- Spyware-	- Malware matching group game- Paired research on prevention strategies and peer presentation	-OneNote and Class Presentation - CrowdStrike Threat Report:

			Ransomware- Prevention strategies	-Know It All Ninja -Class Assessments	https://go.crowdstrike.com/global-threat-report-2024.html- Comparitech UK Ransomware Stats: https://www.comparitech.com/blog/information-security/
	A1.2.2 Hacking – commercial, government, individuals	- Understand different motivations and targets of hacking (commercial, government, individuals).- Identify common hacking techniques: phishing, DoS/DDoS, database breaches.- Analyse hacker profiles: motivations, methods, targets.- Present findings on types of hackers and threats posed.	Motivations of hacking, phishing, DoS/DDoS, database breaches, hacker profiles (hacktivist, cybercriminal, state-sponsored, insider)	- Whole class instruction teaching and learning introduction.- Small group activity: Hacker profile analysis.- Groups research, create, and present hacker profiles.- **Know It All Ninja Quizzes- Class assessments**	- PowerPoint slides, OneNotes, AAQ Information Technology Text Books- Article: Motivations of a Hacker
	A1.2.3 Sabotage – commercial, government, individuals, terrorism	- Define sabotage and differentiate from other cyber threats.- Identify sabotage types targeting commercial, government, individual, terrorism-related systems.- Analyse sabotage scenarios and impacts.- Suggest protective measures and draft defence plans for sabotage prevention.- Present sabotage impact analyses and defence strategies.	Sabotage, data tampering, system destruction, malware insertion, national security legislation	- Whole class instruction teaching and learning introduction.- Small group sabotage scenario analysis.- Individual activity: Sabotage defence planning.- **Know It All Ninja Quizzes- Class assessments**	- PowerPoint slides, OneNotes, AAQ Information Technology Text Books- UK Government Factsheet: Sabotage National Security Bill- Research Paper: Great-Power Offensive Cyber Campaigns
	A1.2.4 Social-engineering techniques used to obtain secure information by deception	- Explain social engineering and psychological tactics.- Identify social engineering methods: phishing, smishing, pretexting, baiting.- Create infographics explaining techniques, warning signs, and avoidance.- Display or submit infographics for feedback.	Social engineering, phishing, smishing, pretexting, baiting	- Whole class instruction teaching and learning introduction.- Individual activity: Create a warning infographic on a social engineering technique.- **Know It All Ninja Quizzes- Class assessments**	- PowerPoint slides, OneNotes, AAQ Information Technology Text Books- Article: 10 Types of Social Engineering Attacks- Social Engineering Awareness Kit

	A1.2.5 Physical security	- Explain importance of physical security in cybersecurity.- Identify common physical security breaches.- Conduct physical security walk-through and evaluate measures.- Discuss pros and cons of physical security methods.- Propose security improvements with justifications.	Physical security, tailgating, forced entry, device theft, CCTV, biometric systems	- Whole class instruction teaching and learning introduction.- Whole class activity: Physical security walk-through.- Pair activity: Think-pair-share on security measures.- Individual activity: Security improvement proposal.- **Know It All Ninja Quizzes- Class assessments**	- PowerPoint slides, OneNotes, AAQ Information Technology Text Books- Article: Physical Security and Cybersecurity- Physical Security video series
	A1.3.1 Operational loss	- Introduce the concept of operational loss in cyber security.- Explain how operational loss affects organisation functionality through security incidents disrupting manufacturing, service, and data.- Use examples such as system downtime, service interruptions, productivity impacts.- Analyse a case study (Colonial Pipeline ransomware attack) discussing causes, impacted operations, response, and recovery.- Understand sector-specific impacts.	Operational loss, system downtime, service availability, productivity impact, ransomware, DoS attack	Whole class instruction and case study analysis.**Know It All Ninja Quizzes, Class assessments**	Class presentations, Class OneNotes, AAQ Information Technology Text BooksCase study: Colonial Pipeline Ransomware Attack
	A1.3.2 Financial loss	- Introduce financial loss from cyber incidents (direct and indirect).- Discuss causes such as service disruption, data breaches, theft, fines.- Explain financial impacts: lost profits, insurance costs, compensation, legal penalties.- Individual risk assessment and reflection on financial loss prevention.- Propose strategies to mitigate financial loss.- Understand the role of financial loss mitigation in cyber security strategy.	Financial loss, data breach, insurance, compensation, legal penalties, risk assessment	Whole class instruction and individual activity.**Know It All Ninja Quizzes, Class assessments**	Class presentations, Class OneNotes, AAQ Information Technology Text BooksArticles: World Economic Forum, IMF
	A1.3.3 Reputational loss	- Explain reputational loss from cyber incidents.- Discuss impacts on public image, trust, credibility, customer loyalty, media coverage, market share.- Develop a reputational recovery plan for a hypothetical	Reputational loss, public image, customer trust, recovery plan, data breach	Whole class instruction and individual activity.**Know It All Ninja Quizzes, Class assessments**	Class presentations, Class OneNotes, AAQ Information Technology Text BooksCase study:

		cyber incident.- Reflect on reputation importance and cyber security role in trustworthiness.			Reputational repercussions
	A1.3.4 Intellectual property loss	- Introduce intellectual property (IP) and cyber threats.- Use interactive threat modelling for IP protection.- Brainstorm IP types (software code, product designs) and threats (hacking, theft, leaks).- Conduct gallery walk on IP protection methods (encryption, access control, NDAs, tracking).- Class discussion on effectiveness of IP protection.	Intellectual property (IP), encryption, NDAs, threat modelling, hacking, employee theft	Whole class instruction and interactive activities.**Know It All Ninja Quizzes, Class assessments**	Class presentations, Class OneNotes, AAQ Information Technology Text BooksArticle: Teaching IP Through Interactive Methods
	A1.4.1 National Cyber Security Centre (NCSC) UK	- Introduce NCSC and its role in UK cyber security.- Explain NCSC resources and guidance.- Emphasise training benefits for staff awareness and skills.- Guide learners through NCSC training topics: passwords, phishing, device security.- Learners complete NCSC Cyber Security Training independently and reflect on applications.	National Cyber Security Centre (NCSC), cyber resilience, training, phishing, password security	Whole class instruction and individual training.**Know It All Ninja Quizzes, Class assessments**	Class presentations, Class OneNotes, AAQ Information Technology Text BooksTraining link: NCSC Cyber Security Training
	A1.4.2 National Institute of Standards and Technology (NIST) USA	- Introduce NIST and its cyber security standards.- Explain the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).- Interactive modelling of NIST functions for a hypothetical organisation.- Independent research on NIST resources.- Class discussion comparing NIST and UK cyber security standards.- Reflect on international collaboration benefits in cyber security.	NIST, Cybersecurity Framework (CSF), Identify, Protect, Detect, Respond, Recover	Whole class instruction, individual research, class discussion.**Know It All Ninja Quizzes, Class assessments**	Class presentations, Class OneNotes, AAQ Information Technology Text BooksResource: NIST Cybersecurity Framework
	A1.4.3 Open Web Application Security Project (OWASP)	- Introduce OWASP and its mission to improve software security.- Explain OWASP Top 10 web application security risks.- Group research and presentation on assigned OWASP Top 10 risks.- Discuss real-world examples and threats.- Establish baseline understanding of web app vulnerabilities.	OWASP, Top 10, injection attacks, authentication, security misconfiguration	Whole class instruction and group activity.**Know It All Ninja Quizzes, Class assessments**	Class presentations, Class OneNotes, AAQ Information Technology Text BooksOWASP links: Main site, Top 10

LA (2) Vulnerabilities	**A2.1.1 Network (vulnerabilities)**	- Introduce and explain network vulnerabilities and their importance. - Identify common vulnerabilities like open ports, weak firewall, unpatched software. - Model vulnerabilities on network diagrams. - Mitigate network vulnerabilities through paired brainstorming. - Research and report on a specific network vulnerability with real-world examples and mitigation strategies.	Network vulnerabilities, Open ports, Firewall, Unpatched software, Access control	- Think-pair-share activity on mitigation strategies. - Individual research report on a network vulnerability including examples and mitigation recommendations. - Know It All Ninja quizzes - Class assessments	Heimdalsecurity - Common Network Vulnerabilities, EC-Council - Network Security Threats and Vulnerabilities, Class presentations, Class OneNotes, AAQ Text Book
	A2.1.2 Organisational (vulnerabilities)	- Explain organisational vulnerabilities from internal processes and human factors. - Identify risks from weak access controls and policies. - Analyse real-world incidents caused by internal vulnerabilities. - Develop improved access control policies in small groups.	Organisational vulnerabilities, Access control, Password policy, Security culture, Multi-factor authentication	- Small group problem-solving task: revise access control policy to address weaknesses. - Know It All Ninja quizzes - Class assessments	CISA Advisory - Weak Security Controls and Practices, Class presentations, Class OneNotes, AAQ Text Book
	A2.1.3 Software (vulnerabilities)	- Explain software vulnerabilities, risks from untrustworthy sources and unpatched systems. - Use real-world zero-day exploit examples to understand threats. - Track current software vulnerabilities in a journal.	Software vulnerabilities, Malware, Zero-day exploit, Patch management	- Pair activity researching a famous zero-day exploit and summarising its impact and mitigation. - Individual ongoing journal entries tracking new vulnerabilities, risks, and mitigation advice. - Know It All Ninja quizzes - Class assessments	Splashtop - Risks and Vulnerabilities of Unpatched Software, SoftwareLab - Zero-Day Exploit Examples (2024), Class presentations, Class OneNotes, AAQ Text Book
	A2.1.4 Operating system, GUI and CLI (vulnerabilities)	- Explain OS vulnerabilities including outdated systems and security misconfigurations. - Understand differences in GUI and CLI vulnerabilities. - Create awareness posters on OS vulnerabilities.	Operating system vulnerabilities, GUI, CLI, Patching, Security settings	- Individual poster creation to educate on a chosen OS vulnerability, including risks and protection measures. - Know It All Ninja quizzes - Class assessments	Sternum IoT - Operating System Vulnerabilities, Class presentations, Class OneNotes, AAQ Text Book
	A2.1.5 Mobile devices reliant on OEM updates (vulnerabilities)	- Explain OEM control of software updates and risks of delays or lack of updates. - Use lifecycle timeline to understand update phases and associated risks. - Debate update vs upgrade decisions.	Mobile devices, OEM, Software updates, End-of-support, Lifecycle	- Small group debate on whether to update, upgrade, or continue using outdated mobile devices, presenting pros and cons. - Know It All	Android Authority - Phone Update Policies, Class presentations, Class OneNotes, AAQ Text Book

				Ninja quizzes - Class assessments	
	A2.1.6 Physical (vulnerabilities)	- Identify physical vulnerabilities affecting device security. - Understand security risks from poor physical practices. - Create quick guide cards for physical security best practices.	Physical security, Device theft, Unattended devices, USB security	- Class tour of mock stations identifying physical vulnerabilities and discussing implications. - Individual creation of "quick guide" cards listing tips to avoid physical vulnerabilities. - Know It All Ninja quizzes - Class assessments	Charter Global - Physical Security Threats & Vulnerabilities, Class presentations, Class OneNotes, AAQ Text Book
	A2.1.7 Process of how people use the system (vulnerabilities)	- Recognise human-factor vulnerabilities from improper system use. - Analyse scenarios involving risky user behaviour. - Develop user checklists for safe system use. - Reflect on personal device/system use for security awareness.	Human factors, Phishing, Password sharing, Security awareness	- Whole class discussion on "spot the vulnerability" scenarios. - Pair activity creating "Think before you click" checklists. - Individual journal tracking daily interactions with systems and identifying risky behaviour with suggestions for safer actions. - Know It All Ninja quizzes - Class assessments	APMG - Security Awareness and Behaviour Explained in 5 Minutes, Class presentations, Class OneNotes, AAQ Text Book
	A2.1.8 Security implications of cloud computing and IoT devices	- Explain key security issues in cloud and IoT technologies- Identify common vulnerabilities such as poor encryption, insecure firmware, and lack of patching- Suggest mitigation strategies	Cloud computing, IoT, encryption, patching, third-party provider, firmware, data interception	**Group Scenario Analysis**: Learners work in small groups to analyse given cloud/IoT scenarios. Each group identifies risks, discusses impact (e.g., data breach), and suggests at least two realistic solutions. Each group presents findings to the class, followed by peer discussion and Q&A. Know It All Ninja quizzes - Class assessments	**Fortinet Cyberglossary: "Top IoT Device Vulnerabilities"** – Highlights IoT risks such as weak authentication, no built-in security, and patching issues.https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities

					Class presentations, Class OneNotes, AAQ Text Book
	A2.2 Where to find vulnerability information	- Identify reliable sources of vulnerability information- Compare key features of NVD, CVE, OWASP- Describe scenarios for using each source	CVE, NVD, OWASP, vulnerability database, zero-day	**Pair Comparison Task**: Each pair selects two vulnerability sources (e.g., NVD vs. OWASP). Learners evaluate update frequency, usability, and content scope. They write a comparison report and share a short presentation with the class to highlight strengths, weaknesses, and recommended usage. Know It All Ninja quizzes - Class assessments	**NIST NVD Database** – Official US government resource for cataloguing vulnerabilities, including severity scoring and patch info.https://nvd.nist.gov **CVE List** – Assigns public IDs to known vulnerabilities with summaries for fast identification.https://www.cve.org Class presentations, Class OneNotes, AAQ Text Book
	A2.3.1 Attack vectors: Wireless	- Describe types of wireless attacks (e.g., Evil Twin)- Explain how these attacks work and how to prevent them- Apply knowledge to real-world scenarios	Evil Twin, WPA3, Bluetooth eavesdropping, rogue access point, sniffing	**Two-Part Task**:1. *Group Scenario Analysis*: Groups are given a wireless attack type and must create a scenario showing how it could occur and the risks involved.2. *Paired Research & Presentation*: Pairs investigate wireless protections (e.g., MAC filtering, VPNs) and create a class best-practices poster. Know It All Ninja quizzes - Class assessments	**Codecademy: "Wireless Attacks"** – Explains wireless hacking methods with simple diagrams.https://www.codecademy.com/article/wireless-attacks**Dig8ital Blog: "Wireless Security 101"** – Practical guidance on securing wireless networks in homes and businesses.https://dig8ital.com/post/wireless-security-101

					Class presentations, Class OneNotes, AAQ Text Book
	A2.3.2 Attack vectors: Internet connection	- Identify how different internet connections (e.g., fibre, 5G) can be exploited- Map risks associated with modems, routers, and ISPs- Suggest mitigation techniques	5G, optical fibre, router spoofing, packet sniffing, DNS hijacking	**Threat Mapping Project**: In groups, learners are assigned an internet connection type (e.g., 5G or home Wi-Fi). They create a threat map showing vulnerabilities, attack methods, and protections. They then present and explain their visual diagram to the class. Know It All Ninja quizzes - Class assessments	**CISA Report: "Potential Threat Vectors to 5G Infrastructure"** – Details cyber attack paths specific to modern network technologies like 5G.https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf Class presentations, Class OneNotes, AAQ Text Book
	A2.3.3 Attack vectors: Internal network access devices	- Identify how routers, switches, and access points are exploited- Describe vulnerabilities like outdated firmware or misconfiguration- Propose hardening methods	Internal network, router, switch, firmware, hardening, access point	**Pair Task – Device Hardening Plan**: Pairs choose one device (e.g., router). They research vulnerabilities and write a hardening plan with steps like disabling ports or updating firmware. They then submit a short report explaining why each step matters. Know It All Ninja quizzes - Class assessments	**CrowdStrike: "What Are Attack Vectors?"** – Introduces how attackers exploit common internal devices.https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/attack-vector/**BusinessTechWeekly: "Network Hardening Best Practices"** – Outlines specific steps to secure hardware and infrastructure.https://w

					ww.businesstechweekly.com/cybersecurity/network-security/network-hardening/ Class presentations, Class OneNotes, AAQ Text Book
	A2.4 Vulnerability assessment tools and methods	- Describe common tools such as port scanners, mappers, and web scanners- Explain what vulnerabilities each tool detects- Evaluate real-world use cases	Port scanner, vulnerability scanner, Nmap, Nessus, registry checker	**Two-Part Task**:1. *Group Research Presentation*: Each group is given one tool and must research its purpose, capabilities, and real-world usage, including a case study.2. *Pair Presentation*: Pairs compare tools and explain scenarios where each is most useful. Peer Q&A follows. Know It All Ninja quizzes - Class assessments	**BrightSec Blog: "Vulnerability Assessment Tools – Key Features"** – Provides tool comparisons and use case examples, including screenshots.https://brightsec.com/blog/vulnerability-assessment-tools-key-features-and-5-tools-you-should-know/ Class presentations, Class OneNotes, AAQ Text Book
	A2.5 Use of independent third-party reviews	- Explain why third-party review of security designs is essential- Identify key security standards and certifications- Evaluate how certification impacts trust	ISO/IEC 27001, SOC 2, due diligence, audit, certification	**Three-Part Task**:1. *Paired Research*: Learners explore ISO 27001 or SOC 2 and list steps and benefits of achieving it.2. *Class Share*: Each pair shares findings via a mini-presentation or poster.3. *Individual Reflection*: Learners reflect on how third-party reviews prevent oversights and build confidence in systems.	**Pivot Point Security** – Offers detailed descriptions of certification and review services, including examples of audit processes.https://www.pivotpointsecurity.com/services/network-architecture-review/ Class presentations, Class OneNotes, AAQ Text Book

				Know It All Ninja quizzes - Class assessments	
	A2.6 Penetration testing and OWASP Top 10	- Describe what penetration testing involves- Identify OWASP Top 10 threats like SQL injection or XSS- Plan how to test for vulnerabilities using these threats	OWASP Top 10, SQL Injection, Cross-site Scripting (XSS), penetration test, red team	**Group Project – Simulated Pen Test Plan**: Groups are assigned a fictional company. They design a basic pen test plan using at least 3 OWASP Top 10 threats (e.g., test SQL injection). Each group presents their test plan, explains test steps, and outlines expected outcomes (e.g., exploit success/failure). Know It All Ninja quizzes - Class assessments	**StationX: "OWASP Top 10 for Pen Testing"** – Breaks down how to test for each OWASP risk with practical techniques and tools.https://www.stationx.net/owasp-top-10-penetration-testing/ Class presentations, Class OneNotes, AAQ Text Book
	A2.7 Passive risk management measures	- Identify and explain passive strategies (transfer, avoid, accept)- Describe benefits and limitations of each- Evaluate when each strategy is appropriate	Risk transfer, risk acceptance, insurance, outsourcing, risk avoidance	**Two-Part Task**:1. *Paired Cost-Benefit Analysis*: Pairs research one passive risk measure and present a cost vs. benefit breakdown using a real or hypothetical case.2. *Individual Reflection*: Learners reflect on risk tolerance in organisations and when passive strategies might be favoured. Know It All Ninja quizzes - Class assessments	**TwProject Blog: "Risk Response Strategies"** – Includes examples of risk transfer, avoidance, and acceptance in business and IT contexts.https://twproject.com/blog/risk-response-strategies-mitigation-transfer-avoidance-acceptance/ Class presentations, Class OneNotes, AAQ Text Book
A3 Legal responsibilities	**A3 Legal responsibilities**	- Understand current legislation relevant to cybersecurity and data protection (GDPR, Computer Misuse Act 1990). - Explain how legislation applies to organisational operations. - Compare key principles and objectives of	GDPR, Computer Misuse Act 1990, data protection, unauthorised access, consent, data	- Whole-class questioning during introduction. - Pair activity: compare GDPR and Computer Misuse Act; present and discuss. - Written summary or short	- CMS Expert Guide on UK Data Protection and Cybersecurity Laws (https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-

		GDPR and the Computer Misuse Act. - Recognise implications of legal compliance.	minimisation, legal compliance	quiz on key legislative differences. - Class discussion reflection notes.	protection-and-cyber-security-laws/united-kingdom) - ICO Data Protection Self Assessment checklist (https://ico.org.uk/for-organisations/advice-for-small-organisations/checklists/data-protection-self-assessment) Class presentations, Class OneNotes, AAQ Text Book
	A3.3.1 General Data Protection Regulation (GDPR)	- Describe core GDPR principles and legal bases for data processing. - Understand consequences of GDPR non-compliance. - Analyse real-world GDPR case studies. - Discuss practical compliance challenges and preventative measures.	GDPR, data privacy, consent, lawfulness, fairness, transparency, data breach, sanctions, data subject rights	- Pair activity analysing GDPR breach case studies. - Group presentation on violations and compliance strategies. - Written reflections on GDPR's impact. - Quiz focused on GDPR principles and legal bases. - Class discussion to deepen understanding. Know It All Ninja quizzes - Class assessments	- ICO Case Studies and Examples (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/case-studies-and-examples/) Class presentations, Class OneNotes, AAQ Text Book
A4 Software and hardware security measures	**A4.1.1 Physical security measures**	- Understand the importance of physical security in protecting organisational assets. - Identify physical security tools and their applications. - Evaluate physical security needs for different organisational contexts. - Research and explain specific physical security technologies.	Physical security, biometric scanners, CCTV, locks, card entry systems, RFID, tailgating prevention, access control	- Small group scenario activity to identify physical security needs and propose solutions. - Pair research and presentation on specific physical security technologies. - Individual reflective journal	- Guide to Physical Security: Controls, Tools, and Examples (https://www.lenels2.com/en/news/insights/the-ultimate-guide-to-physical-security.html) - Avigilon Physical Security Planning and

		- Reflect on integration of physical and IT security.		on physical security impact. - Class discussions and peer feedback after presentations. Know It All Ninja quizzes - Class assessments	Measures Guide (https://www.avigilon.com/blog/physical-security-guide) Class presentations, Class OneNotes, AAQ Text Book
	A4.1.2 Data storage, data protection and backup, and recovery procedures	- Explain the importance of data storage and protection. - Describe different backup types and recovery strategies. - Design backup plans for various organisational scenarios. - Discuss risks of inadequate backup and recovery procedures.	Data storage, data protection, backup types (full, differential, incremental), recovery procedures, onsite/offsite/cloud backup	- Small group activity to design a backup and recovery plan tailored to an organisation. - Group presentations with justification of backup strategy. - Class peer review and discussion on backup strategy suitability. - Quiz or short written test on backup types and concepts. Know It All Ninja quizzes - Class assessments	- Acronis Comparison Guide: Incremental vs Differential vs Full Backup (https://www.acronis.com/en-us/blog/posts/incremental-differential-backups) - Video: Incremental, full and differential backups explained (https://www.youtube.com/watch?v=o-83E6levzM) Class presentations, Class OneNotes, AAQ Text Book
	A4.1.3 Antivirus software and detection techniques	- Describe antivirus software roles and detection methods. - Identify and explain key detection techniques (signature-based, heuristics, file integrity checks). - Research antivirus features and limitations. - Reflect on maintaining antivirus effectiveness.	Antivirus software, malware, signature-based detection, heuristics, quarantine, real-time scanning, sandboxing, updates	- Pair research and presentation on specific antivirus features. - Individual reflective journal on antivirus importance and best practices. - Whole-class discussion on malware evolution and antivirus challenges. - Quiz on antivirus detection techniques. Know It All Ninja quizzes - Class assessments	- How Antivirus Works (https://antivirus.comodo.com/blog/computer-safety/how-antivirus-works/) - Microsoft Defender Antivirus advanced technology overview (https://learn.microsoft.com/en-us/defender-endpoint/adv-tech-of-mdav)

					Class presentations, Class OneNotes, AAQ Text Book
	A4.1.4 Software and hardware firewalls and filtering techniques	- Explain firewall types and their roles in network security. - Describe core filtering techniques (packet filtering, stateful inspection, application layer filtering). - Apply firewall rules to protect a network. - Reflect on real-world firewall breaches and importance of configuration.	Firewalls, software firewall, hardware firewall, packet filtering, stateful inspection, application layer filtering, firewall rules	- Pair activity creating firewall rules for a fictional business. - Peer review and revision of firewall rule sets. - Individual quiz on firewall types and filtering methods. - Written reflection on applying firewall knowledge in real-world scenarios. - Class discussion on firewall breaches and lessons learned. Know It All Ninja quizzes - Class assessments	- Palo Alto Networks: Types of Firewalls Explained (https://www.paloaltonetworks.com/cyberpedia/types-of-firewalls) - Stateless vs Stateful Packet Filtering Firewalls (https://www.geeksforgeeks.org/stateless-vs-stateful-packet-filtering-firewalls/) Class presentations, Class OneNotes, AAQ Text Book
	A4.1.5 User authentication	- Understand authentication concepts and factors. - Explain single-factor and multi-factor authentication (MFA). - Develop personal secure authentication plans. - Reflect on strengths and weaknesses of authentication methods.	Authentication, knowledge factor, possession factor, inherence factor, multi-factor authentication (MFA), security tokens, biometrics	- Individual creation of a personal authentication plan. - Reflective journal discussing chosen methods and security benefits. - Whole-class discussion on organisational authentication considerations. - Short quiz on authentication factors and MFA concepts. Know It All Ninja quizzes - Class assessments	- NCSC Guidance on Choosing Authentication Methods (https://www.ncsc.gov.uk/guidance/authentication-methods-choosing-the-right-type) Class presentations, Class OneNotes, AAQ Text Book
	A4.1.6 Access controls and restricting user access	- Explain access control concepts and models (DAC, RBAC, Rule-Based). - Apply access control models to organisational scenarios. - Define user roles and permissions for access control.	Access control, Discretionary Access Control (DAC), Role-Based Access Control (RBAC), Rule-	- Small group activity planning access control for different organisations. - Group presentation and justification of access control choices.	- Twingate Blog: Access Control Models Explained (https://www.twingate.com/blog/other/access-control-models)

		- Understand importance of access controls in security risk reduction.	Based Access Control, user roles, permissions	- Class Q&A and peer feedback. - Quiz on access control models and applications. - Written reflection on access control importance. Know It All Ninja quizzes - Class assessments	Class presentations, Class OneNotes, AAQ Text Book
	A4.1.7 Trusted computing	- Define trusted computing and its security aims. - Explain components like Trusted Platform Module (TPM), secure boot, digital certificates. - Discuss benefits and challenges of trusted computing. - Create infographics to explain trusted computing features.	Trusted computing, Trusted Platform Module (TPM), secure boot, digital certificates, system integrity, security vs user control	- Individual infographic creation on a trusted computing component. - Gallery walk to share and discuss infographics. - Reflective class discussion on trusted computing trade-offs. - Short written summary or quiz on trusted computing concepts. Know It All Ninja quizzes - Class assessments	- Trusted Computing Group TPM Summary (https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary) Class presentations, Class OneNotes, AAQ Text Book
	A4.1.8 Finding lost or stolen devices	- Understand methods for locating and securing lost or stolen devices. - Explain use of GPS tracking, remote lock and wipe. - Develop organisational response plans for device loss scenarios. - Investigate device-specific security features. - Reflect on importance of these measures in risk mitigation.	Device tracking, GPS, remote wipe, phone home software, data breach, security response plan, BYOD, selective wipe	- Small group scenario planning for lost laptop with classified info. - Group presentations on response plans. - Class discussion on improving plans and preparation. - Pair activity researching device security features and producing user guides. - Peer review of guides. - Quiz on device security and response protocols. Know It All Ninja quizzes - Class assessments	- Prey Project: Remote Wipe Data Protection Explained (https://preyproject.com/blog/what-is-remote-wipe-and-why-you-might-need-it) - Microsoft Intune Selective Wipe (https://learn.microsoft.com/en-us/mem/intune/apps/apps-selective-wipe) Class presentations, Class OneNotes, AAQ Text Book

	A4.1.9 Device based security	- Explain device-based security features (screen timeouts, auto-lock, encryption). - Understand how device security complements broader IT security. - Compare device security settings across platforms. - Develop personal/device security checklists. - Reflect on user role in device security.	Device security, encryption, auto-lock, screen timeout, biometrics, secure boot, patching, mobile device management (MDM)	- Individual development of device security checklist. - Pair activity comparing device security across OS. - Whole-class discussion on improving device security habits. - Quiz on key device security features and benefits. - Reflective journal on user responsibility in device security. Know It All Ninja quizzes - Class assessments	- NCSC Guide to Mobile Device Security (https://www.ncsc.gov.uk/guidance/mobile-device-security) - Apple iOS Security Overview (https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf) Class presentations, Class OneNotes, AAQ Text Book
	A4.2.1 Storage Encryption	- Understand what storage encryption is and its purpose to secure data at rest.- Identify and explain types of storage encryption (file-level, disk-level, database).- Understand AES standard and compare encryption methods.- Analyse real-world examples of data protection through encryption.	Storage encryption, AES, file-level encryption, full-disk encryption, encryption key	- Whole class instruction with Q&A.- Individual activity: Create a detailed comparison table for encryption methods (covering description, strengths, limitations, and typical use cases).- Follow-up quiz (Know It All Ninja) to check understanding.- Class discussion on case studies of device loss/theft and encryption impact.	- OWASP Cryptographic Storage Cheat Sheet: Comprehensive guidelines on cryptographic storage, encryption algorithms, key management, and best practices (https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html).- Veritas File Encryption Overview: Explains file encryption methods, AES and RSA algorithms, and practical applications for securing data (https://www.veritas.com/en/aa/information-center/file-encryption).-

					Class presentation slides covering encryption basics and examples.- Class OneNote with supplementary notes and research links.
	A4.2.2 Communications Encryption	- Explain communications encryption and its role in protecting data in transit.- Describe common protocols: TLS, SSL, VPN, end-to-end encryption.- Identify real-world applications like HTTPS and messaging apps.- Evaluate and select encryption methods appropriate to given scenarios.	Communications encryption, TLS, SSL, VPN, end-to-end encryption, HTTPS	- Whole-class introduction with examples.- Individual activity: Produce a comparison table for communication encryption methods (including purpose, strengths, and common applications).- Small group scenario planning: Groups select suitable encryption for scenarios (remote work, public Wi-Fi, sensitive email), prepare and present their solutions.- Know It All Ninja quizzes and class assessments.	- Cloudflare's "What is end-to-end encryption?": Detailed explanation of E2EE and its importance for secure communications (https://www.cloudflare.com/en-gb/learning/privacy/what-is-end-to-end-encryption/).- Enterprise Networking Planet article on encryption types and use cases: Explains different protocols and their roles in securing communications (https://www.enterprisenetworkingplanet.com/security/encryption-types/).- Class presentation and detailed case examples.- OneNote repository for student notes and research.
	A4.3.1 MAC Address	- Describe MAC address filtering and SSID hiding as wireless security techniques.- Explain how each method restricts or	MAC address filtering, SSID hiding, Wi-Fi	- Whole-class introduction and discussion.- Pair activity: Write a short report	- Article: "MAC Address Filtering and Hiding SSID Won't

	Filtering & SSID Hiding	obscures network access.- Analyse advantages, limitations, and practical effectiveness.- Write and peer-review reports on these methods.- Relate techniques to real-world Wi-Fi security.	security, network access control	summarising the methods, their pros/cons, and real-world examples.- Peer review exchange focusing on report quality and completeness.- Revised report submission.- Class quiz and assessment reflections.	Protect Your Wi-Fi Network" – Discusses limitations and why these are insufficient security measures (https://smallstep.com/blog/mac-address-filtering-and-hiding-ssid-dont-work/).- PCWorld article: "5 Wi-Fi Security Myths You Must Abandon Now" addresses common misconceptions about wireless security (https://www.pcworld.com/article/447974/5-wi-fi-security-myths-you-must-abandon-now.html).- Class presentation slides with real case studies.- OneNote with assignment guidelines and research links.
	A4.3.2 Wireless Encryption	- Understand wireless encryption and its necessity for network security.- Explain WPA2 and WPA3 standards, WPS, and risks of unsecured access points.- Discuss recent breaches caused by weak wireless security.- Collaborate in jigsaw groups to research and teach key wireless encryption topics.	Wireless encryption, WPA2, WPA3, WPS, unsecured access points, network breaches	- Whole-class teaching introducing concepts.- Small group jigsaw activity: Each group researches one topic (WPA2, WPA3, WPS, vulnerabilities) and then teaches peers.- Group presentations.- Formative assessment through class participation.- Follow-up quiz and reflection journals.	- Kaspersky article: "WEP, WPA, WPA2 and WPA3: Differences and Explanation" offers clear comparison of wireless protocols and security features (https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa).- Recent news

					case studies of wireless breaches provided in class.- Class presentation and OneNote resources for further reading.- Video tutorials on wireless security protocols.
	A4.4 Security Issues During Network and System Design	- Recognise importance of designing security into systems from the start.- Understand key principles like “least privilege” and “expect attacks.”- Identify common security standards (e.g., ISO 27000).- Analyse famous data breaches and suggest improvements.- Design secure network systems and communicate design rationale.- Reflect on security design principles through podcasts and journals.	Network security design, least privilege, ISO 27000, risk management, data breaches	- Whole-class lecture with real-life breach examples.- Small group network design challenge: create secure network designs tailored to a hypothetical organisation, including encryption and compliance considerations.- Group presentations with peer feedback.- Pair podcast creation explaining security design principles.- Individual reflection journal on security design lessons.- Know It All Ninja quizzes and class assessments.	- Codecademy case studies: Analyses of major data breaches and lessons learned (https://www.codecademy.com/article/case-studies-notable-breaches).- eSecurity Planet article: Best practices and tools for network security architecture (https://www.esecurityplanet.com/networks/network-security-architecture/).- U.S. Department of Defence Network Infrastructure Security Guide: Authoritative guide to secure network design and configuration (https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF).-

					Class presentations, OneNote resources, and podcast guidelines.
B1 Network Types	**B1.1.1 - B1.1.2 Network Types & Private Networks**	- Define LAN, WLAN, WAN, SAN, PAN, intranet, extranet, cloud networks. - Discuss uses, advantages, disadvantages, and cyber security implications.	LAN, WLAN, WAN, SAN, PAN, intranet, extranet, cloud networks, cyber security risks	- Mind map group activity on network types covering definitions, use cases, advantages/disadvantages, security. - Group presentation and peer Q&A.	- Types of Computer Networks - Too Abstractive - GeeksforGeeks Network Types
	B1.1.3 Wired and Wireless Integration	- Explain Ethernet standards (802 family), wired and wireless integration basics. - Identify compatibility issues and integration challenges. - Evaluate security vulnerabilities unique to integration.	Ethernet 802 standards, wired network, wireless network, integration, signal interference, IP management, security risks	- Small group activity analysing integration scenarios: compatibility issues and solutions. - Pair research on security vulnerabilities (e.g., spoofing, encryption). - Presentations on findings.	- Advantages & Disadvantages Wired vs Wireless - Too Abstractive - GeeksforGeeks Wired and Wireless Networking
	B1.1.4 Schematic Diagrams	- Explain logical and physical network diagrams and their uses. - Create and analyse diagrams with network components and addressing.	Network schematic, logical diagram, physical diagram, IP addressing, port numbers, troubleshooting	- Group activity: complete missing elements in diagrams. - Pair activity: troubleshoot faulty diagrams. - Individual: design a network diagram for a small office, including IP and ports, with a write-up.	- How to Create a Network Diagram - Miro - Network Diagrams Guide - Nulab
	B1.1.5 Features/Requirements of Networks (Cyber Security)	- Identify essential secure network features: scalability, compatibility, performance, backups, fault tolerance. - Explain how these relate to security.	Scalability, compatibility, performance, backup management, fault tolerance, reliability, network security	- Small group: analyse case study network setup for security weaknesses and suggest improvements. - Presentation and peer feedback.	- What is Network Security? - Fortinet
	B1.2.1 Physical Topologies	- Describe star, extended star, hierarchical, mesh, ad-hoc topologies. - Analyse pros/cons including fault tolerance and security implications.	Star, extended star, hierarchical, mesh, ad-hoc, fault tolerance, monitoring, network vulnerabilities	- Group research on assigned topology's security strengths/weaknesses. - Presentation/infographic creation. - Pair scenario: select topology based on business needs and justify choice.	- Network Topologies Explained - Comparitech

	B1.2.2 Logical Topologies	- Define logical topologies (bus, ring). - Explain data flow and security implications in logical topologies.	Logical bus, logical ring, data flow, network security, fault tolerance, monitoring	- Individual research on real-world network using logical bus or ring topology. - Written reflection linking topology to security and efficiency.	- Difference Physical vs Logical Topology - GeeksforGeeks
	B1.3 Network Architecture	- Explain peer-to-peer, client/server, thin client architectures. - Discuss typical uses and security considerations.	Peer-to-peer, client/server, thin client, data access control, vulnerability, monitoring, fault tolerance	- Group research by architecture type: strengths, weaknesses, common security challenges, mitigation. - Presentation/poster creation and Q&A.	- Client Server Architecture - RedSwitches
	B1.4.1 Virtualisation	- Define virtualisation concepts: segmentation, isolation, sandboxing, containerisation. - Explain security benefits and risks of virtual environments.	Virtualisation, segmentation, isolation, sandboxing, containerisation, virtual machines, containers	- Group case study analysis on virtualisation use in industries, discussing segmentation, security benefits, risks. - Pair research on virtualisation platforms' security features and vulnerabilities. - Present findings.	- Containerisation & Cybersecurity - CompTIA - Virtualisation vs Containerisation - GeeksforGeeks
	B1.4.2 Cloud Computing	- Explain cloud computing fundamentals: data storage, scalability, accessibility. - Discuss cloud security risks (data leaks, API vulnerabilities).	Cloud computing, data storage, scalability, API security, data encryption, multi-factor authentication	- Individual infographic creation showing cloud security best practices: MFA, encryption, audits, secure API management.	- Cloud Security Issues - CrowdStrike
	B1.4.3 BYOD (Bring Your Own Device)	- Understand BYOD benefits and risks. - Discuss real-world BYOD security challenges. - Develop a BYOD policy balancing access and security.	BYOD, data leakage, privacy, policy enforcement, antivirus, VPN, device encryption	- Small group: draft a BYOD policy for a given sector covering risks and controls. - Class brainstorming on BYOD security do's and don'ts. - Group presentations.	- BYOD Policies for Organisations - Dashlane
B2 Network components	**B2.1.1 End-user devices, with**	- Explain the role of end-user devices in a network environment, including connectivity (Wi-Fi, Bluetooth, cellular) and processing	End-user devices, connectivity (Wi-Fi, Bluetooth, cellular),	- Know It All Ninja quizzes on device types and security.- Class discussion and	- End User Device Strategy: Security Framework & Controls

	connectivity and processing	capabilities.- Identify types of end-user devices (smartphones, laptops, tablets, IoT devices).- Analyse security implications and measures specific to different devices.- Understand how devices interact within a network.	processing power, IoT devices, security measures (biometric authentication, encryption).	presentations on group findings about device vulnerabilities and security.- Pair activity presentation of comparison charts.- Written reflections on security frameworks for end-user devices.	(UK Government PDF)- Device Security Guidance (NCSC website)- Visual aids showing device interconnectivity and security features.- Classroom presentation slides.- Interactive group activity worksheets.
	B2.1.2 Connectivity devices	- Describe the purpose and function of connectivity devices (switches, routers, modems, access points, hubs).- Understand how these devices impact network security, performance, and scalability.- Analyse security configurations and recommend improvements.	Connectivity devices, switches, routers, modems, access points, hubs, security configurations, firewall, default passwords.	- Group presentations on device functions and security risks.- Pair security evaluation reports and recommendations.- Individual written summaries of multi-functional device pros and cons.- Quizzes covering device roles and security.	- Network Devices: Common Types and Their Functions (Lepide blog)- Physical devices or simulated software demos.- Security configuration guidelines for routers and switches.- Classroom demonstration kits.- Research templates for individual activity.
	B2.1.3 Connection media	- Identify and describe types of connection media: physical (Ethernet, USB, optical fibre) and wireless (Wi-Fi, NFC, Bluetooth, cellular 5G).- Explain advantages, typical uses, and security risks of each.- Propose security measures tailored to each media type.	Connection media, Ethernet, Wi-Fi, Bluetooth, NFC, cellular, optical fibre, network performance, security vulnerabilities, mitigation techniques.	- Group research presentations analysing media types, risks, and protections.- Individual reports evaluating a chosen media's security risks and mitigation strategies.- Class discussion participation.- Quizzes on media types and security.	- Network Connected Security Technologies (NCST) Guidance (NPSA)- Types of Transmission Media (GeeksforGeeks)- Visual aids illustrating media types.- Case study handouts.- Security mitigation strategy templates.
	B2.2 Application and	- Explain common uses and security risks of external media (USB drives, external HDDs,	External media, malware, encryption,	- Pair research presentations on encryption and secure	- Cyber Security and External Storage

	security issues of external media and storage	SD cards).- Understand risks such as malware, data interception, and data loss.- Research encryption methods and secure disposal techniques.- Conduct risk assessments and propose security measures for external media.	secure disposal, data interception, data loss prevention, device management.	disposal.- Individual risk assessment reports with mitigation strategies.- Class discussion on best practices.- Quizzes on external media security risks.	Devices Risks (Beyond20 blog)- Security Best Practices for Removable Media (Hackernoon article)- Visual diagrams of data breach scenarios.- Research guides and assessment templates.- Encryption tool tutorials.
	B2.3.1 Network and device operating systems	- Describe the purpose and types of network and device OS (Windows Server, Linux, macOS, Android).- Compare GUI and CLI interfaces.- Identify OS vulnerabilities and suggest mitigation methods.- Create security checklists for chosen OS environments.	Operating systems, network OS, GUI, CLI, patching, default settings, security patches, user permissions, firewall.	- Group case study presentations on OS vulnerabilities.- Individual OS security checklist creation.- Quizzes on OS features and security concepts.- Class discussions reflecting on security best practices.	- Network Operating System (NOS) overview (Network Encyclopedia)- OS security checklist templates.- Vulnerability case studies.- Demo videos on GUI vs CLI usage.- Security patching guidelines.
	B2.3.2 Network monitoring, management and troubleshooting tools	- Explain the role of monitoring and troubleshooting tools in network security and performance.- Identify common tools (Wireshark, vulnerability scanners, performance monitors).- Create a basic network troubleshooting plan.	Network monitoring, troubleshooting, Wireshark, vulnerability scanner, performance monitoring, intrusion detection.	- Individual network troubleshooting plan.- Class quiz on monitoring tools and purposes.- Group discussion on real-world troubleshooting examples.- Practical demonstrations of tool usage.	- 20 Best Network Monitoring Tools for 2024 (Comparitech)- Network Troubleshooting Guide for IT Professionals (Auvik)- Software demo access (Wireshark etc.).- Troubleshooting plan templates.- Video tutorials on tool usage.
	B2.3.3 Network applications	- Understand the role of network applications in communication, collaboration, and data management.- Explain functions of VPNs,	Network applications, VPN, remote desktop,	- Group scenario analysis and presentations on network app security.- Pair comparisons of	- What is Application Security? (Imperva)- Security in Network

		remote desktops, databases, email servers, VoIP.- Identify security considerations (access control, encryption, data integrity).- Analyse security risks and mitigation measures in network applications.	database, access control, encryption, data integrity, email servers, VoIP.	communication applications and their security.- Quizzes on application security concepts.- Class discussions on best practices.	Design (Cisco blog)- Case studies of network applications.- Access to collaboration and communication apps for demos.- Security framework documents.- Presentation and worksheet materials.
	B2.3.1 – Network and Device Operating Systems	- Describe the purpose of network and device operating systems (managing hardware, supporting applications, providing user interfaces).- Compare GUI and CLI, identifying their uses in management and security.- Identify differences between NOS (e.g. Windows Server, Linux) and device OS (e.g. Windows, Android).- Investigate vulnerabilities in OS and suggest mitigation strategies.- Develop a personal checklist for securing an operating system.	- Network Operating System (NOS)- Device Operating System- GUI (Graphical User Interface)- CLI (Command Line Interface)- Patch- Firewall- Permissions- Default settings- Vulnerabilities	- **Group Task**: Analyse an OS vulnerability case study; identify cause, impact, and mitigation. Present findings to class.- **Individual Task**: Create a personal OS security checklist covering updates, permissions, firewalls, etc., with explanations.- **Knowledge Check**: Quizzes on OS types and roles.- **Know It All Ninja quizzes, Class assessments**	- **Class presentations, Class OneNotes**- Network Encyclopaedia – NOS- Example case studies on OS vulnerabilities- Screenshots or demos comparing GUI and CLI- Security checklist templates
	B2.3.2 – Network Monitoring, Management and Troubleshooting Tools	- Explain the purpose of network monitoring, management and troubleshooting tools.- Identify tools such as Wireshark, performance monitors, and vulnerability scanners.- Describe how tools are used to detect and resolve network issues.- Create a network troubleshooting plan for a common issue.	- Network monitoring- Troubleshooting- Performance monitor- Wireshark- Vulnerability scanner- Bottlenecks- Connectivity issues- Intrusions	- **Individual Task**: Create a troubleshooting plan for a network issue. Include symptoms, tools used, and step-by-step resolution.- **Knowledge Check**: Class discussion and short quiz on monitoring tools.- **Know It All Ninja quizzes, Class assessments**	- **Class presentations, Class OneNotes**- 20 Best Network Monitoring Tools – Comparitech- Network Troubleshooting Guide – Auvik- Sample troubleshooting templates- Demonstration of tools (e.g. Wireshark)
B3 Networking infrastructure	**B3.1.1 TCP/IP**	– Describe the purpose of the TCP/IP protocol suite. – Explain how data is broken into packets and transmitted across layers. – Identify how error correction and reliability	TCP/IP model (4 layers), packets, IP addressing, protocols, data	– Practical activity configuring TCP/IP settings on devices or simulators. – Short written explanation of	– **TCP/IP Model Overview** (GeeksforGeeks): https://www.geeksforge

services and resources		are handled. – Configure basic TCP/IP settings and use basic network diagnostic tools.	integrity, configuration, ping, ipconfig	packet flow through TCP/IP layers. – Know It All Ninja quizzes. – Class knowledge check questions.	eks.org/tcp-ip-model/ – **TCP/IP Packet Format** (GeeksforGeeks): https://www.geeksforgeeks.org/tcp-ip-packet-format/ – Class presentations – Class OneNotes – Network simulation tool (e.g., Packet Tracer or NetSim)
	B3.1.2 Ports	– Explain the function of ports in networking. – Identify well-known ports and their uses. – Understand how services are mapped to specific port numbers.	Ports, IP addressing, protocols, well-known/registered/dynamic ports (e.g., HTTP – 80, HTTPS – 443)	– Research task on assigned ports (purpose and security implications). – Group presentation and class discussion. – Know It All Ninja quizzes.	– **What is a Computer Port?** (Cloudflare): https://www.cloudflare.com/en-gb/learning/network-layer/what-is-a-computer-port/ – Port number reference sheets – Class presentations – Class OneNotes
	B3.1.3 Packet	– Define a data packet and its structure. – Distinguish between TCP, UDP, and IP packets. – Understand headers, payloads, and error handling.	Packet structure, TCP vs UDP, payload, headers, trailers, fragmentation, error detection	– Group activity identifying components in example packets. – Worksheet comparing TCP and UDP. – Know It All Ninja quizzes. – Short-answer written assessment.	– **Data Packet Anatomy** (TechRepublic): https://www.techrepublic.com/article/exploring-the-anatomy-of-a-data-packet/ – **TCP vs UDP Comparison** (FreeCodeCamp): https://www.freecodecamp.org/news/tcp-vs-udp/ – Wireshark (optional demo or screenshots) – Class

					presentations – Class OneNotes
	B3.1.4 NAT	– Explain how NAT works and why it's used. – Compare types of NAT (static, dynamic, PAT). – Explore IPv4 and IPv6 structures and their relation to NAT. – Recognise and classify IP address ranges.	NAT, IP masking, IPv4/IPv6, static/dynamic NAT, PAT, private IP addresses (RFC 1918), special IP addresses	– Group activity comparing NAT types. – Paired IP addressing task: convert and identify IP range type. – Individual written summary of NAT purpose and impact. – Know It All Ninja quizzes.	– **What is NAT?** (Fortinet): https://www.fortinet.com/resources/cyberglossary/network-address-translation – **Types of NAT** (GeeksforGeeks): https://www.geeksforgeeks.org/types-of-network-address-translation-nat – **Special IP Addresses** (BinaryTerms): https://binaryterms.com/special-ip-addresses-in-ipv4.html – Class presentations – Class OneNotes
	B3.2 Domains, Sub-domains & Segmentation	– Explain the role of domains, sub-domains, and segmentation. – Identify how segmentation supports trust relationships and access control. – Create basic domain models that represent a segmented network.	Domains, sub-domains, trust relationships, segmentation, access control, containment, hierarchical structures	– Group diagram task on domain segmentation. – Paired analysis of segmentation case studies. – Individual design of segmented network. – Know It All Ninja quizzes.	– **Network Segmentation Guide** (PhoenixNAP): https://phoenixnap.com/blog/network-segmentation – **OWASP Network Segmentation Cheat Sheet**: https://cheatsheetseries.owasp.org/cheatsheets/Network_Segmentation_Cheat_Sheet.html – Class presentations – Class OneNotes
	B3.3 Application of	– Identify and explain the role of network infrastructure devices. – Understand how	Router, switch, firewall, bridge,	– Short research task: students complete a network device	– **Network Devices Overview**

	Network Devices	each device contributes to security and network configuration. – Recognise best practices in securing and deploying devices.	gateway, server, WAP, device security, access control, configuration	chart. – Individual task: create a network security checklist. – Know It All Ninja quizzes.	(GeeksforGeeks): https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/ – Manufacturer datasheets (e.g., Cisco, Netgear) – Class presentations – Class OneNotes
	B3.4.1 DNS	– Describe how DNS resolves domain names into IP addresses. – Use tools to perform DNS and reverse lookups. – Explain caching and its effects.	DNS, domain name resolution, recursive/resolver servers, root servers, reverse DNS, DNS cache	– Paired activity using `nslookup`, `dig` or online tools. – Worksheet identifying steps in DNS resolution. – Know It All Ninja quizzes.	– **What is DNS?** (Cloudflare): https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/ – **DNS Lookup Tool** (MX Toolbox): https://mxtoolbox.com/DNSLookup.aspx – **Reverse DNS Tool** (MX Toolbox): https://mxtoolbox.com/ReverseLookup.aspx – Class presentations – Class OneNotes
	B3.4.2 Directory Services & IAM	– Understand what directory services and IAM do in a network. – Compare different DS technologies (e.g., AD, OpenLDAP). – Recognise best practices in access management (e.g., MFA, least privilege).	Directory services, identity and access management (IAM), authentication, authorisation, multi-factor authentication, least privilege, auditing	– Individual activity: Create a one-page guide on DS/IAM security best practices. – Research task comparing two directory service technologies. – Know It All Ninja quizzes.	– **IAM Overview (Microsoft)**: https://www.microsoft.com/en-gb/security/business/security-101/what-is-identity-access-management-iam – **IAM Fundamentals (Microsoft Learn)**: https://learn.microsoft.c

					om/en-us/entra/fundamentals/introduction-identity-access-management – Class presentations – Class OneNotes
	B3.4.3 Authentication services	- Explain the role of authentication in securing systems.- Compare types of authentication (SFA, TFA, MFA, SSO).- Describe and evaluate protocols (PAP, CHAP, EAP).- Apply knowledge to real-world business scenarios.	Authentication, SFA, TFA, MFA, SSO, PAP, CHAP, EAP, network security	- Group presentations on authentication methods.- Protocol comparison summaries.- Individual report: protocol application and improvements in a business setting.- Know It All Ninja quizzes, Class assessments.	- NCSC guide on authentication: ncsc.gov.uk- ID R&D authentication overview: idrnd.ai- Class presentations, Class OneNotes
	B3.4.4 Dynamic Host Configuration Protocol (DHCP)	- Describe the role and benefits of DHCP in network management.- Differentiate between static, dynamic, and automatic IP allocation.- Configure DHCP settings based on network requirements.	DHCP server/client, IP address, dynamic/static/automatic allocation, lease time, IP range	- Group simulation: design DHCP configuration.- Group explanation of configuration decisions.- Know It All Ninja quizzes, Class assessments.	- DHCP overview video: YouTube- Microsoft DHCP documentation: learn.microsoft.com- CloudNS article on DHCP: cloudns.net- Class presentations, Class OneNotes
	B3.4.5 Routing	- Explain the function of routing in networks.- Compare static and dynamic routing.- Identify routing protocols (RIP, OSPF, BGP) and their uses.- Analyse routing tables for optimisation.	Static routing, dynamic/adaptive routing, IGP, EGP, BGP, routing table, RIP, OSPF	- Routing table analysis in groups.- Protocol comparison in pairs with class sharing.- Know It All Ninja quizzes, Class assessments.	- AWS routing overview: aws.amazon.com- Routing protocol examples and diagrams- Class presentations, Class OneNotes
	B3.4.6 Remote access services	- Explain the purpose of remote access in businesses.- Describe dial-up and VPN methods.- Evaluate security and usability of each method.- Understand the connection handshake process.	Remote access, VPN, dial-up, handshake, encryption, secure tunnelling	- Pair comparison: dial-up vs VPN.- Class discussion on relevance and security.- Know It All Ninja quizzes, Class assessments.	- HPE remote access overview: hpe.com- Diagrams of handshake/authentication process- Class

					presentations, Class OneNotes
	B3.5.1 File and print services	- Describe file and print services and their management.- Explain file access control and printer management.- Design an access control policy for a fictional organisation.	File server, print server, access control, print queue, printer drivers	- Individual activity: design access control policy and flowchart.- Written justification of design choices.- Know It All Ninja quizzes, Class assessments.	- PaperCut guide to print servers: papercut.com- Brainscape flashcards: brainscape.com- Class presentations, Class OneNotes
	B3.5.2 Web, mail and communication services	- Describe how web, mail, and communication services operate.- Identify and explain the use of protocols (HTTP, HTTPS, SMTP, POP).- Analyse risks and benefits of data sharing.- Evaluate encryption and vulnerability issues.	HTTP, HTTPS, SMTP, POP, encryption, vulnerabilities, protocols, communication services	- Individual report: impact of communication services on business and security.- Discussion on protocol strengths/risks.- Know It All Ninja quizzes, Class assessments.	- Protocol explanations: whatismyipaddress.com - Real-world examples of protocol use- Class presentations, Class OneNotes
C1 Internal policies	**C1.1.1 Cyber Security Policy (PDCA Model – ISO 27001:2013)**	- Describe the purpose and structure of a cyber security policy based on ISO 27001.- Explain how PDCA applies to cyber security.- Design a cyber security policy using the PDCA cycle.- Evaluate strengths and weaknesses in password policies.	ISO 27001, PDCA (Plan-Do-Check-Act), continuous improvement, policy enforcement	- Group presentations of PDCA-based policy designs.- Peer-assessed analysis of real-world password policies.- Self-assessment of understanding through reflective writing.- Quiz on PDCA cycle and ISO 27001 concepts.	- ISO 27001 Overview Video- PDCA Cycle Video 1- PDCA Cycle Video 2- ISO PDCA Cycle Article- ISO 27001 Toolkit- Case studies from IT Governance
	C1.1.2 Security Audits and Compliance	- Explain the purpose of security audits.- Describe steps of an audit process.- Create an audit compliance checklist.- Develop a flowchart for an audit process.	Audit goals, compliance, checklist, gap analysis, audit scope	- Group-created checklists peer-reviewed through fictional scenarios.- Individual audit process flowchart submission assessed against rubric.- Class quiz on audit principles and goals.- Written reflection on the importance of audit compliance.	- Comparitech Security Audit Guide- SafetyCulture Audit Checklist Tool- Editable audit templates for group work- Teacher-created audit scope visual diagram
	C1.1.3 Backup Policy	- Describe components of a robust backup policy.- Compare different backup types and	Full, incremental, differential,	- Comparison presentations graded via peer feedback	- MSP360 Backup Policy Best Practices-

		their applications.- Design a backup schedule based on business needs.- Demonstrate understanding via flowcharts and infographics.	continuous backups, storage media, backup testing	sheet.- Flowchart assessment for process completeness and accuracy.- Infographic assessed via design rubric focused on clarity, role identification, and compliance points.- Short quiz on backup types and their benefits.	DarwinsData Backup Guide- Backup flowchart templates (editable)- Sample business scenarios for schedule planning
	C1.1.4 Data Protection Policy	- Define data protection and explain its purpose.- Identify the responsibilities of a DPO.- Outline a staff training module for compliance.- Understand the importance of accountability and privacy.	GDPR, Data Protection Officer (DPO), privacy rights, data handling, compliance	- Learner-created training module outline assessed using criteria for relevance, coverage, and clarity.- Class discussion contributions on GDPR and staff responsibilities.- Written reflection on staff training's role in compliance.	- Data Protection Officer Role Guide- GDPR training templates- Sample privacy policies for analysis- Editable module planning template
	C1.1.5 Cyber Security Incident Response Policy	- Explain the components of an incident response policy.- Describe roles and responsibilities during a cyber incident.- Create a checklist for incident closure and reporting.	Incident response, escalation, legal notification, documentation, roles and responsibilities	- Group role tables assessed for role clarity and alignment with real-world protocols.- Incident closure checklists marked for completeness and logical sequence.- Scenario-based quiz on incident response procedures.	- Crowdstrike Incident Response Framework- Incident Response Flowchart- Example incident logs- Sample press release templates for PR protocol discussion
	C1.1.6 Disaster Recovery Policy	- Explain the purpose of disaster recovery policies.- Identify roles and protocols during disaster events.- Create flowcharts and checklists for response planning.	Disaster categories, triage, BCP (Business Continuity Plan), communication protocols, recovery	- Group presentations of disaster response flow diagrams with rubric-based peer and teacher evaluation.- Pair work checklists reviewed for completeness, accuracy, and realistic role assignment.- Individual reporting template reviewed using marking criteria on clarity and scenario coverage.	- Cloudian Disaster Recovery Guide- Disaster Recovery YouTube Video- Incident planning templates- Real-world disaster case studies for analysis

	C1.1.7 External Services Policy	- Explain the purpose of external service policies.- Identify accountability and compliance issues.- Develop process maps and support checklists.- Understand the risk of third-party services.	SLA (Service Level Agreement), authorisation, vendor accountability, external service risks, compliance	- Group-created policy process maps peer-assessed for flow and content.- Pair comparison tables on cloud standards assessed on accuracy and research depth.- Service support checklists reviewed for clear escalation and documentation steps.- Class quiz on SLA elements and external risk factors.	- Guidance for Engaging Cloud Service Providers- MSP360 SLA Guide- SLA examples- Risk assessment templates for third-party services- Cloud provider T&Cs for comparison activity
D1 Forensic collection of evidence	**D1.1.1 Meeting requirements for forensics**	- Describe key steps in handling digital evidence (isolation, power state, chain of custody).- Apply forensic protocols to hypothetical scenarios.- Explain the use of digital forensic tools and their limitations.	Forensic procedure, chain of custody, evidence contamination, device isolation, disk imaging, malware analysis, system log	- Group presentation of confiscation protocols with peer feedback.- Paired infographic on forensic tools evaluated through presentation and Q&A.- Individual analysis of system logs using a data table; teacher-marked for accuracy and relevance.	- **ACPO Good Practice Guide for Digital Evidence**: Detailed official standards for evidence handling Link- **SANS Digital Evidence Collection Article**: Contemporary best practice summary Link- Class presentations, Class OneNotes, Sample system logs, Infographic templates
	D1.1.2 The challenges of live forensics	- Explain the concept and importance of live forensics.- Identify risks of data alteration and strategies to preserve volatile data.- Plan methods for recovering or analysing live data safely.	Live forensics, volatile data, memory dump, data corruption, integrity, live capture tools	- Group-developed strategy for live data capture and recovery presented and peer-reviewed.- Learners complete a worksheet identifying risks and mitigation methods from a simulated case.- Written reflection task on when live forensics is essential.	- **Vaia Explanation – Live Forensics**: Overview of key concepts and best practices Link- Teacher-developed case studies for simulation- Class presentations, Class OneNotes, Live forensics planning templates

	D1.1.3 Network forensics	- Describe the process of network forensic investigation.- Differentiate between passive and active scanning.- Evaluate the importance of authorisation and risk planning.- Create response plans to malware or alert scenarios.	Network traffic, passive scanning, active scanning, log files, malware response, firewalls, permissions	- Class quiz during video walkthrough to test understanding.- Group authority briefing assessed for clarity, completeness, and risk awareness.- Individual written malware response plan marked against a checklist of expected steps.	- **Wireshark Tutorial**: YouTube- **Network Logs with Event Viewer**: YouTube- Sample malware scenarios, Log samples for review- Class presentations, Class OneNotes
	D1.1.4 Documenting the scene	- Describe and apply procedures for documenting digital incident scenes.- Create and interpret scene plans, sketches, and notes.- Construct checklists for future incident response.	Scene documentation, contemporaneous notes, scene plans, digital photography, sketching, witness statement	- Group project: simulated scene documentation including visual and written materials.- Class feedback session on quality of documentation.- Individual checklist assessed against key forensic documentation standards.	- **College of Policing – Securing a Digital Scene**: Link- **NIJ Guide to Photographing and Sketching Scenes**: PDF- **CPS Guidelines on Witness Statements**: Link- Scene simulation materials (photos, props), Checklist templates, Class presentations, Class OneNotes
D2 Systematic forensic analysis of a suspect system	**D2.1.1 Retaining snapshots of the system**	- Understand the importance of accurate system snapshots- Practice creating and verifying hashes- Describe imaging and data preservation techniques	System imaging, bit-by-bit copy, hash function, checksums, RAM, virtual machines, deleted files	- Group presentations on data preservation methods- Paired hash creation task with integrity checks- Quiz on importance of data integrity- Know It All Ninja quizzes, Class assessments	- Class presentation- Sample files for hashing- Forensic imaging software simulation- OneNote task pages- https://www.geeksforgeeks.org/digital-evidence-preservation-digital-forensics/
	D2.1.2–D2.1.3 Recording	- Explain chain of custody- Design procedures to document evidence handling-	Chain of custody, evidence	- Group-designed chain of custody flowchart- Pair analysis of forensic reports-	- Class presentation- Sample forensic reports- Templates for

	findings and alterations	Distinguish between intentional and unintentional alterations	admissibility, integrity, reliability	Reflective journal on use of originals vs copies- Know It All Ninja quizzes, Class assessments	chain of custody documentation- OneNote reflective journal page- https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-chain-custody
	D2.1.4 Visual evidence of findings	- Capture screenshots and visual documentation with metadata- Understand role of metadata in supporting claims	Visual evidence, screenshots, photos, metadata, timestamps	- Group practical visual evidence task with written reports- Paired metadata analysis and presentation- Know It All Ninja quizzes, Class assessments	- Mock forensic scenarios- Sample files with metadata- Screenshot tools- Metadata viewer software- https://www.ironhack.com/gb/blog/metadata-forensics-when-files-can-speak-and-reveal-the-truth
	D2.1.5 Relevance of evidence and false positives	- Recognise false positives- Define relevant search criteria- Understand risks of misclassification	False positives, relevance, file signatures, filtering	- Group activity defining relevance criteria- Short written explanation on reducing false positives- Class discussion with case study reflections- Know It All Ninja quizzes, Class assessments	- Simulated file lists (relevant/irrelevant files)- Case studies on real-world false positives- Class presentation- https://solicitorsnortheast.co.uk/false-positives-in-digital-evidence-ruining-peoples-lives/
	D2.2.1 Provide evidence of a crime/incident	- Classify forensic findings into categories- Link findings to legal and organisational impacts	Incident classification, regulatory breach, civil liability, cyber-attack, negligence	- Group case analysis presentations- Pair presentations on real-life consequences- Individual infographic mapping categories and impacts- Know It All Ninja quizzes, Class assessments	- Real or fictional forensic case studies- Templates for incident mapping- Tools for infographic creation (e.g. Canva)- https://www.ncsc.gov.u

					k/information/categorising-uk-cyber-incidents
	D2.2.2 Show internal/external compromise	- Identify indicators of system compromise- Differentiate between internal and external threats	Indicators of compromise (IoC), DNS logs, DDoS, login anomalies	- Group network log analysis- Individual infographic summarising indicators of compromise- Know It All Ninja quizzes, Class assessments	- Simulated logs with anomalies- Network flow diagrams- Visual resources on traffic patterns- https://www.microsoft.com/en-gb/security/business/security-101/what-are-indicators-of-compromise-ioc
	D2.3.1 Prevent recurrence of incidents	- Recommend remediation actions- Structure reports to highlight procedural weaknesses	Incident reports, remediation, procedural errors, recommendations	- Paired report outline with peer review- Marked structured report draft (formative assessment)- Know It All Ninja quizzes, Class assessments	- Sample incident reports- Report templates- Case scenarios to base reports on- https://www.dataguard.co.uk/blog/how-soon-after-an-incident-should-you-write-a-report/
	D2.3.2 Improve IT policies	- Identify policy gaps- Propose updates aligned to modern cyber threats	IT policy, MFA, data protection, outdated procedures	- Group presentations of gap analysis- Pair proposals with written justifications- Know It All Ninja quizzes, Class assessments	- Sample outdated IT policies- NCSC BYOD guidance- Policy writing templates- https://clickup.com/blog/it-policies-and-procedures/

	D2.3.3 Improve security protection measures	- Analyse categories of security protection- Recommend specific improvements for identified weaknesses	Physical security, software, hardware, training, procedural security	- Group presentations on specific security category improvements- Peer feedback and refinement task- Know It All Ninja quizzes, Class assessments	- Security design case studies- NCSC security culture guidance- Templates for improvement plans- https://www.npsa.gov.uk/security-culture- https://www.ncsc.gov.uk/collection/cyber-security-design-principles
Unit 4 Relational Database Development					
Specification References	**Topic Area: Main Items**	**Outcomes that students should be able to**	**Key Terms / Concepts (literacy)**	**Assessment**	**Resources**
LAA	**A1: Relational Database Management Systems**	- Define key database terms- Explain the structure and purpose of relational databases- Compare desktop and server databases- Interpret and draw Entity-Relationship Diagrams (ERDs)- Understand relational keys and integrity constraints- Use relational algebra symbols to query databases	Data, Database, Table, Record, Field, Attribute, Tuple, Relation, Domain, Cardinality, Super key, Candidate key, Primary key, Foreign key, Entity integrity, Referential integrity, ER diagrams, One-to-one, One-to-many, Many-to-many, Relational algebra (Union, Intersect, Join, Select)	- Short-answer questions on database structure and terminology- Label and explain elements of an ER diagram- Class task: Draw ER diagrams from scenario-based descriptions- Know It All Ninja quizzes- Class assessments on database fundamentals	- **Class presentations, Class OneNotes**- Data.gov.uk – sample datasets- Teach-ICT – ERD resources- TechTarget – Server vs Desktop databases- ComputerScience.GCSE.Guru- Database software (e.g. Microsoft Access, MySQL)
	A2: Manipulating Data Structures and Data in	- Explain the purpose of manipulating data- Create, update, delete and retrieve records using a database- Use GUI and SQL to build and run queries- Understand the purpose and structure of reports	Update, Delete, Append, Retrieve, Query, Report, SQL, Criteria, Multi-table queries, GUI	- Practical database task: Use GUI to create queries- Extension: Use SQL to run queries across multiple tables- Peer feedback on report	- **Class presentations, Class OneNotes**- Sample databases- ComputerScience.GCSE.Guru- Data.gov.uk –

	Relational Databases		(Graphical User Interface), Data redundancy	design- Know It All Ninja quizzes- Class assessments on query functionality	real-world datasets- Microsoft Access or equivalent
	A3: Normalisation	- Identify problems in un-normalised databases- Explain the purpose of normalisation- Apply 1NF, 2NF, and 3NF to data- Create ERDs from normalised tables- Define referential integrity and identify violations- Create a data dictionary including keys and data types	1NF, 2NF, 3NF, Functional dependency, Insertion anomaly, Deletion anomaly, Update anomaly, Entity, Relationship, Referential integrity, Orphan record, Data dictionary, Composite key	- Worksheet: Normalise datasets from UNF to 3NF- Draw ERDs from normalised tables- Scenario task: Identify referential integrity violations- Create a data dictionary- Know It All Ninja quizzes- Class assessments on data modelling	- **Class presentations, Class OneNotes**- LearnLearn.uk – Normalisation walkthroughs- ADA Computer Science- Kaggle & Data.gov.uk – datasets- Spreadsheet or Access for manipulation
	A4: Planning a Relational Database Solution in Response to a Client Brief	- Define the purpose of a database system- Research existing solutions and technical requirements- Plan a database using appropriate terminology- Explain and sequence the stages of development- Identify the structure and vocabulary needed for documentation	Database planning, Client brief, Requirements, Purpose, Research, Logical structure, Technical vocabulary, Feasibility, Project timeline	- Group presentation: Database development process- Written task: Define database requirements from a client scenario- Group task: Produce a flowchart or timeline of development stages- Know It All Ninja quizzes- Class assessments on planning documentation	- **Class presentations, Class OneNotes**- Zibtek.com – Database development cycle- Project planning templates- Visual aids – flowchart and planning tools- Sample briefs/scenarios
	B1: Relational Database Design Techniques and Processes	- Recap and apply key relational database terms and normalisation- Understand the stages of conceptual and logical modelling- Use relational algebra to define relationships and queries- Understand the use of DBMSs and how to select the right implementation tool- Explore database prototyping and testing processes- Evaluate the quality, effectiveness, and appropriateness of database designs	Relation, Attribute, Tuple, Domain, Degree, Cardinality, Super key, Candidate key, Primary key, Foreign key, Composite key, Referential integrity, 1NF–3NF, Conceptual model, Logical model, Relational algebra	- **Starter recap quiz**: Key database terms- **Guest speaker session** (optional): Real-world database design insights- **Whole class discussion**: Conceptual vs logical models and relational algebra- **Mini group project**: Design a database system for a scenario (e.g., vet appointment system), including conceptual and logical models and use of	- **Class presentations, Class OneNotes**- *TutorChase.com* – Schema & relational modelling- *Data.gov.uk* – Real datasets for practice- *DatabaseManagement.Fandom.com* – Server vs local DBMS- *Teach-ICT.com* – Relational algebra resources- Templates for ERD and

			(AND, OR, NOT), DBMS, Server vs Cloud, Prototyping, Testing, Quality, Effectiveness	relational algebra- **Scaffolded templates**: For model building and relational algebra- **Individual research task**: Server vs cloud solutions + summary via comparison charts- **Class presentations**: Students present findings and implementation tool comparisons- **Final discussion**: Evaluate database quality (correctness, integrity, effectiveness of design, normalisation level)- **Know It All Ninja quizzes, Class assessments**	logical models- Database software (MS Access / MySQL / SQLite)
LAB	**B2: Design Documentation**	- Create a comprehensive design specification addressing client needs- Differentiate between brief requirements and client requirements- Consider audience, purpose, legal and ethical factors (e.g., GDPR)- Design data structures (ERD, data dictionary, normalisation)- Design user interfaces with attention to accessibility and usability- Understand and plan for thorough testing- Research and build an implementation plan	Design specification, Brief vs Client requirements, Audience, Purpose, Legal/Ethical (e.g., GDPR), Data dictionary, UI Design, Accessibility, Usability, Form controls (input, calculated, disabled), Testing (functionality, accessibility, usability, integrity), Implementation Plan, Risk Management	- **Whole class discussion**: Key terms in a design specification- **Research activity**: Legal and ethical considerations (data protection laws)- **Paired scenario task**: Create a design specification and data structures for a client brief (e.g., enrolment system)- **Peer review session**: Exchange and critique design documentation- **Modelling task**: Normalisation, ERD, data dictionary- **Whole class critique**: Evaluate example UI designs for good/bad features- **Research task**: Use of form controls (input, calculated, disabled)- **UI**	- **Class presentations, Class OneNotes**- *Microsoft Support* – Database design and templates- *UXPin.com* – UI/UX principles- *ICO.org.uk* – GDPR guidance- *Form control examples* – Demo files (provided in class)- *Implementation plan templates*- Testing checklist template- Access or web-based form builders

				design creation: Students design forms, menus, queries- **Discussion**: What should be tested and when in a database- **Real-world case studies**: Testing failures and lessons- **Research task**: Implementation plan essentials (timescales, team, resources, risks)- **Class presentations**: Students present implementation plans- **Know It All Ninja quizzes, Class assessments**	
	B3: Reviewing and Refining Designs	- Understand the value of involving clients in reviews- Conduct peer and self-reviews to evaluate design quality- Use structured feedback to identify strengths and improvements- Refine and update design documentation based on feedback and reflection	Suitability, Client involvement, Peer review, Self-review, Legal and ethical constraints, Accuracy, Consistency, Feedback loop, Refinement	- **Whole class discussion**: Client involvement in design reviews – advantages/disadvantages- **Discussion**: Key criteria for effective peer and self-review- **Peer review task**: Students review each other's full design specifications and UI elements using guided criteria- **Feedback reflection**: Students evaluate which feedback to act upon and justify choices- **Individual refinement task**: Update and improve their design documentation- **Teacher-led debrief**: Showcase improvements and reflect on the importance of iteration in design- **Know It All Ninja quizzes, Class assessments**	- **Class presentations, Class OneNotes**- *TestSigma.com* – Database testing guidance- *Review checklist templates*- *Peer review forms* – Structured feedback templates- *Example improved design docs* (for modelling best practice)

LAC	**C1: Producing a Database Solution**	- Use a DBMS (e.g., MS Access) to create databases, tables, relationships, and validation rules- Implement database solutions based on a given or created design specification- Write SQL scripts to create and manage databases- Compare GUI-based and SQL-based implementation- Generate queries, reports, and user interfaces- Populate a database using external datasets- Develop and present a complete working database based on a project brief	DBMS, Tables, Primary/Foreign Keys, Relationships, Data Validation, SQL (CREATE, INSERT, SELECT, JOIN), Queries, Reports, Forms, Navigation Forms, UI, Data Importing, Data Cleaning, Prototyping	- **Guided tutorials**: Students follow step-by-step guides in MS Access or SQL-based environments- **Practical tasks**: Students create database structures (tables, keys, validation) from design- **Implementation diary**: Students document challenges and solutions- **SQL scripting task**: Implement same database in SQL and compare with GUI approach- **Discussion**: Evaluate GUI vs SQL – advantages and disadvantages- **Formative practice**: Create reports and queries with increasing complexity- **UI creation task**: Design and build forms with navigation, input validation, and child forms- **Real-world scenario project**: Students implement a full database solution based on a given design brief- **Peer review session**: Evaluate each other's work using a checklist- **Final presentation**: Students explain their design choices and challenges faced- **Know It All Ninja quizzes, Class assessments**	- **Class presentations, Class OneNotes**- MS Access / MySQL / SQLite software- *W3Schools* – SQL tutorials: w3schools.com/sql- *TutorialsPoint* – DBMS and SQL resources: tutorialspoint.com- Example design specifications (vet system, school database)- Data sets (CSV, Excel) for importing and cleaning- UI design checklists and templates- SQL scripts and test files for practice
	C2: Testing the Database Solution	- Understand and apply different types of test data (normal, extreme, erroneous)- Test all parts of the database: tables, queries, forms, reports, UI- Categorise tests: functionality,	Test Data Types, Object Testing, Usability Testing, Functional Testing,	- **Whole class discussion**: Importance of testing and consequences of failure- **Scenario review**: Explore	- **Class presentations, Class OneNotes**- *TestSigma.com* – Effective database

		integrity, performance, usability- Design and carry out usability tests with appropriate users- Create effective user feedback tools (e.g., questionnaires)	Performance, Feedback, Neutral Questioning	real-world database failure examples- **Individual testing task**: Plan and document tests on their own database using all data types- **Testing log**: Record results and changes made- **Peer testing**: Swap databases and create new test scenarios- **Create a test plan**: Include categorised test types- **Usability testing**: Run tests with selected users and collect feedback- **Feedback questionnaire task**: Students design their own feedback forms- **Debrief session**: Students discuss findings and improvements made- **Know It All Ninja quizzes, Class assessments**	testing guides: testsigma.com- Real-world case studies on data failures- Usability testing templates- Feedback questionnaire examples- Test plan and test log templates
	C3: Reviewing the Database Solution	- Evaluate a database solution based on design requirements- Identify legal and ethical issues (e.g., GDPR)- Assess quality, usability, and fitness for purpose- Identify strengths, limitations, and areas for improvement- Use testing evidence and user feedback to support review	Review, Quality, Fitness for Purpose, Client Requirements, GDPR, Ethical Constraints, Feedback, Evidence-based Evaluation	- **Class discussion**: What makes a good database solution?- **Review checklist activity**: Students apply criteria (e.g., functionality, accuracy, accessibility)- **Evidence-based evaluation**: Students refer to test logs and user feedback to support review- **Individual task**: Complete a formal review report highlighting strengths and improvements- **Optional peer review**: Use structured criteria to evaluate a peer's solution- **Class reflection session**: Share lessons learned	- **Class presentations, Class OneNotes**- Review criteria templates- Feedback log examples- Example database solutions (for comparison or critique)- Legal/Ethical guidance from *ICO.org.uk* on GDPR

				and design improvements- **Know It All Ninja quizzes, Class assessments**	
	C4: Optimising the Database Solution	- Understand performance factors: indexing, data types, volume, queries- Refine queries and relationships for performance- Apply optimisation techniques (indexing, query refinement, normalisation)- Evaluate optimisation impact on database performance	Performance, Indexing, Data Volume, Data Types, Query Optimisation, Normalisation, Efficient Joins	- **Class discussion**: What slows down a database?- **Scenario exploration**: Review a poorly performing database- **Checklist-based activity**: Identify bottlenecks in given database or student's own- **Practical task**: Apply indexing, review data types, simplify queries- **Before-and-after analysis**: Students compare performance of original vs optimised database- **Reflection report**: Document optimisation process and outcomes- **Optional challenge**: Optimise a complex provided database- **Know It All Ninja quizzes, Class assessments**	- **Class presentations, Class OneNotes**- Example underperforming database files- *Teach-ICT.com* – Indexing and optimisation techniques- Optimisation checklist templates- Benchmarking tools for testing query speed (in MS Access/MySQL)
Course Work	**Course Work**	Pupils using knowledge from previous learning pupils will need to complete the set brief. Hand in date END OF TERM 3			