Digital Technologies – 9 and 10_ Digital systems

	STRAND	Knowledge and understanding				Processes and production skills																	
		Digital Systems		Representation of data		Collecting, managing and analysing data				*Creating Digital Solutions by:*													
										Investigating and defining		Generating and designing		Producing and implementing		Evaluating		Collaborating and managing					
	Content Description	Investigate the role of hardware and software in managing, controlling and securing the movement of and access to data in networked digital systems (ACTDIK034)		Analyse simple compression of data and how content data are separated from presentation (ACTDIK035)		Develop techniques for acquiring, storing and validating quantitative and qualitative data from a range of sources, considering privacy and security requirements (ACTDIP036)		Analyse and visualise data to create information and address complex problems, and model processes, entities and their relationships using structured data (ACTDIP037)		Define and decompose real-world problems precisely, taking into account functional and non-functional requirements and including interviewing stakeholders to identify needs (ACTDIP038)		Design the user experience of a digital system by evaluating alternative designs against criteria including functionality, accessibility, usability, and aesthetics (ACTDIP039)		Design algorithms represented diagrammatically and in structured English and validate algorithms and programs through tracing and test cases (ACTDIP040)		Implement modular programs, applying selected algorithms and data structures including using an object-oriented programming language (ACTDIP041)		Evaluate critically how student solutions and existing information systems and policies, take account of future risks and sustainability and provide opportunities for innovation and enterprise (ACTDIP042)		Create interactive solutions for sharing ideas and information online, taking into account social contexts and legal responsibilities (ACTDIP043)		Plan and manage projects using an iterative and collaborative approach, identifying risks and considering safety and sustainability (ACTDIP044)	
Sequence of Lessons / Unit	**Approx. time rq'd**	**Year A or B**	CD	Achievement standard #	CD	Achievement standard #	CD	Achievement standard #	CD	Achievement standard #	CD	Achievement standard #	CD	Achievement standard #	CD	Achievement standard #	CD	Achievement standard #	CD	Achievement standard #	CD	Achievement standard #	CD	Achievement standard #
Data security	7	10	☑	1, 2	☐		☐		☐		☐		☐		☐		☐		☐		☑	9	☐		☑	10

Years 7 and 8 Achievement Standard	Years 9 and 10 Achievement Standard	
By the end of Year 8 • Students distinguish between different types of networks and defined purposes. (1) • They explain how text, image and audio data can be represented, secured and presented in digital systems. (2) • Students plan and manage digital projects to create interactive information. (3) • They define and decompose problems in terms of functional requirements and constraints. (4) • Students design user experiences and algorithms incorporating branching and iterations, and test, modify and implement digital solutions. (5) • They evaluate information systems and their solutions in terms of meeting needs, innovation and sustainability. (6) • They analyse and evaluate data from a range of sources to model and create solutions. (7) They use appropriate protocols when communicating and collaborating online. (8)	By the end of Year 10 • Students explain the control and management of networked digital systems and the security implications of the interaction between hardware, software and users. (1) • They explain simple data compression, and why content data are separated from presentation. (2) • Students plan and manage digital projects using an iterative approach. (3) • They define and decompose complex problems in terms of functional and non-functional requirements. (4) • Students design and evaluate user experiences and algorithms. (5) • They design and implement modular programs, including an object-oriented program, using algorithms and data structures involving modular functions that reflect the relationships of real-world data and data entities. (6) • They take account of privacy and security requirements when selecting and validating data. (7) • Students test and predict results and implement digital solutions. (8) • They evaluate information systems and their solutions in terms of risk, sustainability and potential for innovation and enterprise. (9) • They share and collaborate online, establishing protocols for the use, transmission and maintenance of data and projects. (10)	

Topic: Digital systems
Units

Year 9	**Year 10**
Connected via a network : 7 hours Examine different types of networks, protocols and the role of software and hardware plays.	**Data: controlled and secured 7 hours** Explore how data can be secured through access controls, virus checking, and encryption.

Data: controlled and secured
Students should explore how data can be secured through various methods such as access controls, virus checking, encryption, backups, data masking, and data erasure. Examine malicious code such as computer viruses, malware, adware, Trojans and spyware that are used to commit cyber-attacks. As an extension, set up the challenge of designing a secure digital system.

Flow of activities				
Short text	Authorisation Develop an understanding of how digital systems can be restricted to authorised use.	Encryption Examine how information is encoded and how with the relevant 'key' the computer decodes the message.	Malicious code Introduce and examine common types of cybercrime.	Hackers and hacking Set the challenge of designing a secure digital system.
Questions to guide exploration	*What security measures are used to protect digital systems from unauthorised use?*	*How does encryption make the internet safer?*	*How can cyber criminals threaten internet users?*	*What is hacking?*
AC Alignment	*Digital Systems (ACTDIK034)* *Collecting, managing and analysing data (ACTDIP036)*	*Digital Systems (ACTDIK034)* *Collecting, managing and analysing data (ACTDIP036)* *Evaluating (ACTDIP042)*	*Digital Systems (ACTDIK034)* *Collaborating and managing (ACTDIP044)*	*Digital Systems (ACTDIK034)* *Collecting, managing and analysing data (ACTDIP036)* *Collaborating and managing (ACTDIP044)*
What's this about?	Students should develop an understanding of how digital systems can be restricted to authorised use. Authorisation is a key aspect of information security.	Security is a key concern on the internet, especially when sending and receiving sensitive information. A common way of providing information security over the internet is through encryption. Information is encoded and with the relevant 'key' the computer decodes the message. Historical examples are often given to help explain encryption. One such example is the Enigma code, a type of enciphering used by the German armed forces. Alan Turing famously cracked the code.	Cybercriminals use malicious code such as computer viruses, malware, adware, Trojans and spyware to commit cyber-attacks.	Hackers, those that are involved in cybercrime, generally learn how computer systems and networks operate and then use this knowledge to gain unauthorised access to computer systems.
The focus of the learning (in simple terms)	Explore approaches such as passwords, tokens, fingerprint readers, voice recognition, facial recognition and security passcards used to enter buildings with restricted access. Use mobile devices to explore the concept of biometric security – fingerprints used for most mobile phones or facial recognition with Windows Surface Pro-type devices. Voice identification is used by the ATO to authorise users. Why might this form of authorisation be used? Compare and contrast this with other security measures. Discuss why organisations might use email validation when setting up an online account. Brainstorm reasons for internet security and ways the internet is made safer and how we should protect ourselves online. Students could explore RFID (Radio Frequency Identification) emitters and readers to create a secure entry system with an Arduino electronics kit.	Provide examples of encryption and the use of public and private keys to decode. Relate information security threats to people's everyday use of the internet to bank, shop, and access social security, taxation and other personal information. Describe ways encryption and authentication are applied together to create a secure environment.	Introduce common types of cybercrime including viruses, malware, DDOS (Denial-of-service) attacks and phishing scams. List some of the ways cyber attackers trick users into divulging personal information or enabling them to infect their computers with malicious code. In collaborative groups, students define a cybersecurity threat and describe approaches to protect against this type of threat. They could create an advertisement, an infographic with relevant data, or create a new product idea and create a video to market it on Kickstarter. Research some of the emerging careers that are related to cyber security.	Set up the challenge of designing a secure digital system. For example, a business is setting up an online purchasing system. What approaches might be used to ensure customer safety of personal information as well as protecting the organisation against security threats.
Supporting resources and tools and purpose/context for use.	Network Security This lesson plan for Network Security, focuses on authentication, encryption, firewalls and Mac address filtering. Cyber Security Threats This lesson covers the fundamentals of cyber security: methods to detect and prevent cyber-security threats. 'Cybersecurity 101' The internet is fundamentally insecure. However, there are simple things you can do to protect yourself	'The Internet: Encryption & Public Keys' Kid krypto—Public-key encryption A fairly challenging activity to represent encryption using the sending and receiving a secret message as the analogy. 'Cyber Codes' Learn how trustworthy online communication actually is and how encryption can protect your privacy. CS Unplugged: Field guide: Coding – Encryption	Malicious Code This lesson looks at the fundamentals of cyber security and malicious code that includes computer viruses, malware, adware, Trojans and spyware. 'The Internet: Cybersecurity & Crime' This video describes common types of cybercrime including viruses, malware, DDOS attacks and phishing scams. 'How not to get hacked' Great video to discuss hacking and ways to protect yourself from these attacks.	Game of Hacks Online game to develop digital system security understanding. Note considerable programming knowledge required. 'The secret lives of Hackers' Learn the true meaning of hacking and some of the many reasons that hackers hack When children are breached – inside the massive VTech hack This article provides a useful discussion starter about protecting personal information and potential security issues from data breaches.

	and your information. Learn what they are in NOVA's Cybersecurity Lab. NOVA Labs: Cyber security These cyber security short animated videos each have a quick quiz to complete. The videos cover a basic intro into cyber security, hacking and privacy and cyber codes, and there is a game too for students to apply their understandings. Arduino: Security Access Using RFID Reader A tutorial for programming Arduino kits with RFID chips as security devices. Introduction to Cybersecurity Enrol in CISCO's free course.	An online resource for teaching computer science to students, this chapter focusses on coding – encryption. Journey into cryptography An extensive online course on cryptography developed by Khan Academy.	Day of STEM Cyber Security resources	
Assessment	**Suggested approaches may include:** Presentation or demonstration, Adapted worksheet, Artefact analysis, Labelling diagram, Text, Digital capture, Design plan. **Achievement standard** **Explain** the control and management of networked digital systems and the security implications of the interaction between hardware, software and users.	**Suggested approaches may include:** Presentation or demonstration, Adapted worksheet, Artefact analysis, Labelling diagram, Text, Digital capture, Design plan. **Achievement standard** **Explain** the control and management of networked digital systems and the security implications of the interaction between hardware, software and users.	**Suggested approaches may include:** Presentation or demonstration, Adapted worksheet, Artefact analysis, Labelling diagram, Text, Digital capture, Design plan. **Achievement standard** **Explain** the control and management of networked digital systems and the security implications of the interaction between hardware, software and users.	**Suggested approaches may include:** Presentation or demonstration, Adapted worksheet, Artefact analysis, Labelling diagram, Text, Digital capture, Design plan. **Achievement standard** **Explain** the control and management of networked digital systems and the security implications of the interaction between hardware, software and users.