Foxford Learning Plan

YEAR 13

Topic Unit 1: Learning Aim D

Protecting data and information

Spring 2

Key Vocabulary

Threats	A threat is any potential danger to information or systems
Virus	A computer virus is a malicious piece of computer code designed to spread from device to device
Hackers	Anyone who uses their abilities to gain unauthorised access to systems or networks in order to commit crimes
Phishing	Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source
Shouldering	It is a technique used to obtain information such as personal identification numbers
Data Validation	It is the process of checking that the user's input matches the constraints of the system it is being entered into
Data Verification	It is the process of ensuring that the data received is the same as the data sent
Accidental damage	It is unforeseen or unintentional actions that resulted in a loss of function
Malware	This is any type of software created to harm or exploit another piece of software or hardware
File permissions	The authorization given to users that enables them to access specific resources on the network
Anti-virus	A program designed to detect and remove viruses and other kinds of malicious software
Protecting Data	How your personal information is used by organisations, businesses or the government
Security Issues	Unmitigated risk or vulnerability in your system that hackers can use to do damage to systems or data
Firewalls	Software that enforces a set of rules about what data can enter and leave a network
Encryption	Prevents data from being intercepted, is a process data is encoded to prevent unauthorised access
File Permissions	Files and folders stored on your computer can have varying levels of permissions meaning you can decide which users can access each file or folder

Key Skills

Over the course of the topic, I will be able to: -

- Explain data protection and information
- Describe different types of threats
- Explain how to protect files using password
- Differentiate the differences between validation and verification
- Explain types of security issues and solution
- How to prevent network threats
- Describe file permissions
- Specify who and what can read, write, modify, and access file



I will Understand

1. Types of threats
2. How to assign file permission
3. The differences between validation and verification
4. Various threats: malware, virus, worm, trojan and ransomware
5. Different types of malware
6. What network threats are
7. The implication of data threats