GLOSSARY

Term	Definition
Application software	A program containing a set of instructions to the computer that allowsthe user to carry out a specific function.
Artificial Intelligence (AI)	When computers perform tasks normally requiring human intelligence,such as problem solving, adapting according to previous experience.
Augmented reality	The process of superimposing a computer-generated image on a user'sview of the real world.
Authentication	When a user confirms their unique identity on a computer system.
Back-up	A copy of a file that is kept in a location away from the computer whichcan be used to restore data in case of loss.
Biometrics	Technologies that recognise human body characteristics (e.g., fingerprint) to authenticate a person's identity.
Bionics	The science of constructing artificial systems (e.g., limbs) that have someof the characteristics of biological systems.
Bluetooth	A wireless communication protocol for exchanging data over shortdistances.
Cloud computing	Software applications and data that are stored online and used throughthe Internet.
Communication software	A program designed to pass information from one system to another.
Compression	Making files smaller by reducing the number of bits used to store theinformation.
Cookies	Cookies are text files containing small pieces of data that are sent fromthe website you are browsing. They are stored in your computer and provide a way to recognise you and keep track of your preferences.
Cyberbullying	Bullying using digital communication tools such as the Internet or mobilephones.
Data	A collection of text, numbers or symbols in a raw or unorganised form.
Data capture	The process of taking information from a document and converting it intodata which a computer can read.
DDoS	A distributed denial-of-service attack, which is a malicious attempt to disrupt the operation of a service or network by flooding the target with fake traffic.
Digital footprint	The data left behind when you have made an interaction online.

Term	Definition
Drone	A flying robot that can be remotely controlled.
E-commerce	Commercial transactions made electronically on the Internet.
Encoding	The process of converting data from one form to another.
Encryption	The process of scrambling data when it is being sent to protect it from unauthorised users, as they do not have an encryption key to decode it.
Ethernet	The most usual way of connecting computers together in a local areanetwork (LAN).
E-waste	Electronic appliances such as mobile phones, computers, and televisionsthat are thrown away without the intention of re-use.
Expert system	A computer system that stores facts and can search these facts for information according to a set of rules, copying the decision-making abilityof a human expert.
Extranet	An extranet is a controlled private network that is accessible to some authorised users outside of the organisation.
Green IT	Environmentally responsible and eco-friendly use of computers and theirresources in order to reduce the carbon footprint.
Hacking	The gaining of unauthorised access to data in a computer system.
Hardware	The physical components of a computer.
Information	Data that has been processed, normally by a computer, to give it meaning.
Information handling software	The process of gathering, recording and presenting information in a waythat is helpful to others (e.g., in a graph).
Input device	A piece of equipment that transfers data into a computer so it can beprocessed.
Internet	A public worldwide system of computer networks.
Intranet	A private operated network where data content and access is controlled.It is insulated from the global internet.

Term	Definition
Key logging	The use of a computer program to record every keystroke made by acomputer user without their knowledge and usually in order to gain fraudulent access to passwords and other confidential information.
Knowledge	When a person gains information such as facts, or the understanding ofinformation such as how to solve problems.
Local Area Network (LAN)	A network that links computers that are geographically close enoughtogether to be hard wired.
Logical protection	Software security controls put in place to manage access to computersystems (e.g., passwords).
Malware	Short for malicious software, it covers all software that is specifically designed to disrupt, damage or gain unauthorised access to a computer system.
Near-field Communication (NFC)	A set of communication protocols based on a radio frequency (RF) field,designed to exchange data between two electronic devices through a simple touch gesture.
Open source software	Software that is distributed with its source code so that anyone caninspect, modify or enhance it.
Output device	A piece of equipment that receives data from your computer once it hasbeen processed (e.g., a monitor).
Packet sniffing	A computer program or computer hardware that can intercept andmonitor network traffic.
Physical protection	Protecting equipment by physically preventing access to it.
Port	A docking point available for connection to peripherals such as input andoutput devices.
Protocol	A standard set of procedures that allow data to be transferred betweenelectronic devices.
Radio-frequency Identification(RFID)	A technology to record the presence of an object using radio signals.
Ransomware	A type of malware that prevents you from using your computer oraccessing certain files until you pay a ransom to the hacker.
Robotics	The use of robots to perform tasks done traditionally by humans.
Social engineering	When users are tricked into making security mistakes, so they give upconfidential information.
Social network	An online service or site that allows people to communicate with friendson the Internet using a computer or mobile phone.

Term	Definition
Software	The programs that tell a computer what to do.
Spyware	Software that enables a user to obtain information about your computeractivities by transmitting data secretly from your hard drive.
Storage device	A piece of internal or external hardware used for saving, carrying andextracting data from a computer.
System software	A type of computer program that operates a computer's hardware andprovides a platform to run application programs.
Teleworking	When you work at home, while communicating with your office using awide area network (WAN).
Topology	The way in which computers are arranged in a network.
Trojan Horse	A type of malware that is usually disguised as legitimate software used byhackers trying to gain access to your computer system.
USB	An industry standard method of transferring data between a host device(e.g. a computer) and a peripheral device (e.g. a mouse). Stands for Universal Serial Bus.
Utility software	A program designed to help to analyse, configure, optimise or maintain acomputer.
Validation	Checking input to make sure it meets a set of defined rules and is sensiblein order to prevent errors.
Verification	Checking input to make sure that the data entered is identical to theoriginal source in order to prevent errors.
Video conference	An electronic meeting, allowing users to hold face-to-face meetingswithout having to be in the same place physically.
Virtual reality	A computer-generated simulation in which a person can interact within anartificial three-dimensional environment.
Virus	A piece of code which is capable of copying itself and is placed on yourcomputer with the aim of damaging the system.
Wearable technologies	Smart electronic devices that are designed to be worn by the user andhave sensors that collect data such as heart rate.
Wide Area Network (WAN)	A telecommunications network that extends over a large geographicalarea, connecting more than one Local Area Network (LAN).
Wireless	Uses a technology such as radio or microwaves to transmit signals ratherthan using wires or cables.
Worm	A computer program that replicates itself in order to spread maliciouscode throughout your system.