Villa Real School

together we achieve

Information and Communications Technology Policy

2024

Responsibility: Alan Granton		Date: October 2024

Date to be reviewed: October 2027

Introduction

Villa Real school is a forward-thinking vibrant organisation where children will be given the skills and education to prepare them for their next step in life. We provide a caring working atmosphere where your child will be given access to a full and varied curriculum, they will be supported at all times along their learning journey. In this ever increasingly technology focused world, we view ICT and computing as a vital component in readying your child for their future steps.

Rationale

At Villa Real School we are committed to providing your child with an ICT and computing curriculum that will incorporate the four strands of Interactive Media, Computing, Communication Technology and using technology in life, but – most importantly – safety through all four strands. We consider the e-safety aspect a high priority for vulnerable students and will focus on teaching your child relevant ways to stay safe now - as well as in the future. ICT/ Computing will be incorporated across the curriculum to enrich learners' experiences and work towards using technology in different situations.

Aims of ICT and Computing at Villa Real

Our aims are:

- To provide all learners with at least the requirements of the National Curriculum at the appropriate level, that is relevant to their next steps ensuring a wide and varied curriculum accessible by all ages and abilities.
- To develop learners' confidence when using ICT to plan, carry out, review, and improve tasks.
- To equip students to use technology for communication effectively and safely, at school, in work situations and during adulthood.
- To encourage students to use technology as a problem-solving tool
- To use technology to enhance students' learning in other areas, across the curriculum.
- To provide adapted technology and use it effectively to ensure each learner achieves their full potential
- To provide learners with the adult skills they need to carry out everyday tasks using technology, including – where appropriate – electronic payments, using .gov websites, and NHS services
- To provide learners with the knowledge to be safe at all times when using modern technology

Guidelines for teaching

- All students will receive ICT/ Computing lessons – either taught as a stand-alone topic or integrated into other curriculum areas
- Planning will be based on the National Curriculum for ICT, Computing and Interactive Media at the appropriate level for individual students, and to ensure enjoyment, engagement and success in the subject.
- Where appropriate the ICT / Computing lead will support teachers with planning to ensure lessons are suitable for individual learners.
- ICT skills and good practice will be taught and reflected upon in other curriculum areas to help students understand the benefits and limitations of technology
- Evidence of progress will be recorded by a combination of: printed student work, work saved via cloud services, statement evidence, and photographic evidence
- Students should be taught to reflect upon, evaluate, and improve work
- Where appropriate teachers will integrate online safety into lessons.
- Computing will be offered as an enrichment activity to all learners and will offer the opportunity to experience elements of Computing that are not a focus in the curriculum e.g. computer club.

Internet and Online Safety

Internet and online safety forms part of the core curriculum and is embedded through the curriculum whilst also taught as standalone units. Units taught in the safety aspect of the Computing curriculum complement subject matter delivered in Kidsafe, PSHCE and RSE. The views of parents, carers and pupils are taken into account to shape the curriculum whilst the latest advice and guidance is sought from DFE, SWFL and Online 360. Online safety as whole is regularly reviewed by the schools Online Safety Team and monitored by school governors on regular basis.

Internet and Email

Pupils will be protected from having access to undesirable materials by:

- Close adult supervision
- Using only web sites which have recently been checked for content by an adult
- Working on-line, with an understanding that they will be held accountable for their own actions, as outlined in the school Acceptable Use Policy.
- Knowing that if they see something which upsets them that they switch off the monitor and tell an adult.

- For the storage of temporary files, pupils will each have a personal directory on the computer network
- Computers will at all times be ready for use in the classrooms and shared areas
- Hardware and software provision will be reviewed each year
- Training will be made available each year for all school staff according to need
- Appropriate monitoring of systems and procedures will be carried out by the onsite ICT technician. Breaches of the online safety policy will be kept and reviewed by the online safety team.
- Staff will be regularly updated in respect of the latest threats to children's safety.

Equal Opportunities

All pupils will have regular and equal access to a broad and balanced ICT experience across the whole curriculum.

Pupils in primary provision will follow a curriculum which will be supported by the subject specialist and a package known as Purple Mash, Switched On ICT and bespoke resources. Primary students will also have the opportunity to engage in Primary Computing activities based on the Primary National Curriculum for computing. All students will be supported by staff to achieve their personal best in every activity. Those pupils working below the National Curriculum will access the Engagement Model.

Key stage three students will follow a curriculum that supports progression towards qualification route. This will be mapped and supportive to prepare students for potential access to qualification courses. All students will be supported by staff to achieve their personal best in every activity.

Where the above is not appropriate to the learners needs ICT skills for adulthood will be accessed, focusing on stay safe online.

Secondary students will have the opportunity to study for recognised qualifications in either ICT, Interactive Media, Digital Skills, Computer Coding or Computer Science at an appropriate level that is accessible, challenging and engaging. All students will be supported by staff to achieve their personal best in every activity.

Resources

Students will have access to technology that is appropriate to complete tasks set in the curriculum. Access to this technology is given on the understanding that it is used appropriately, and it is at the discretion of the classroom teacher to determine this.

Access to study materials will be available that is suitable for the key stage of students and should be used appropriately in lesson time.

Assessment

Assessment follows the whole school assessment policy of:

- REAL progress against the REAL Curriculum utilising BSquared
- The 'Engagement Model' set by the Department for Education.
- EHCP targets
- Exam board criteria as appropriate
- Purple Mash online teacher assessment.

Homework

The ICT / Computing curriculum follows the whole school policy, while in addition to this allows learners to complete homework using the online platform Purple Mash.

Acceptable Use Policy

Both students and staff members must follow the Acceptable Use Policy when using technology in school. All learners and parents will be provided with access to this policy through the school website.

Appendix 1

Glossary of Key Terms

TERM	DEFINITION
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber-attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.

Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.