Villa Real School

together we achieve

Pupil/Student Acceptable Use Policy 2024

Responsibility: Alan Granton /Andrew Moore   Date: October 2024

Date to be reviewed: October 2026

Acceptable Use Policy

I will only access computing equipment when a trusted adult has given me permission and is present.

I will not deliberately look for, save or send anything that could make others upset.

I will immediately inform a trusted adult or a member of Villa Real staff if I see something that worries me, or I know is inappropriate.

I will keep my username and password secure; this includes not sharing it with others.

I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.

I will always use my own username and password to access the school network and subscription services such as Purple Mash.

In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.

I will respect computing equipment and will immediately notify a trusted adult or member of Villa Real staff if I notice something isn't working correctly or is damaged.

I will use all communication tools such as email and blogs carefully. I will notify a trusted adult or a member of Villa Real staff immediately if I notice that someone who isn't approved by the teacher is messaging.

I will follow the remote learning policy set out by Villa Real School. When taking part in remote learning activities I will be kind and courteous to all involved, including staff, other students and parents. I will always try my best.

I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

I will not take or distribute images of anyone without their permission.

I will immediately report any damage or faults involving equipment or software, however this may have happened.

I understand that work I save is covered by the privacy statement and under GDPR.

Where work is protected by copyright, I will not try to download copies (including music and videos)

When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that if I fail to comply with this acceptable use agreement, I may be subject to investigation. This could include loss of access to the school network/internet contact with parents and in the event of illegal activities involvement of the police.

Before I share, post or reply to anything online, I will T.H.I.N.K.

I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

If I take school electronic equipment home, I will be careful to keep it safe and use it for school work only.

T= is it true?
h= is it helpful?
I = is it inspiring?
N = is it necessary?
K = is it kind?

<u>ELECTRONIC DEVICES, MOBILE PHONE and SMART WATCHES CODE OF CONDUCT</u>

Villa Real School recognises that on some occasions it may be helpful for a pupil/student to bring a mobile phone, an electronic device or smart watch into school, for instance: listening to music, relaxation, to support self-regulation and or if they walk to school unaccompanied or they are being collected by a different parent/carer. We believe that pupil/student use of a mobile phone during the School day can sometimes be inappropriate and this agreement outlines how pupil/student phones and other electronic devices in school will be managed within our school.

<u>OUR PUPIL/STUDENT MOBILE PHONE & ELECTRONIC DEVICES CODE OF CONDUCT</u>

- If a pupil/ student brings a mobile into school, this should be handed to the class teacher to be kept in a secure place until home time
- The School cannot accept responsibility for damage or loss of an electronic device or mobile phone brought into school

- We currently advise that the use of Smart Watches is not appropriate in school due to risks of loss and damage

  However, should you wish for your child to use their Smart Watch during school hours, the texts, emailing and calls facilities must be disabled between the hours of 9.20am – 3.20pm

School staff are responsible that the above is adhered to at all times throughout the hours of the school day.

Parents/carers may want to look at the advice on www.internetmatters.org which explains how to add some parental/carer controls to the phone/electronic device and gives advice on how to keep children safe.

I agree to the guidelines set out in the Pupil/student Electronic Devices and Mobile Phone Code of Conduct 2021.

Pupil/student Name: ______________________________

Parent/carer Name: ______________________________

Date: ______________________________

- As the parent/carer of the pupil/student I know that my child has signed this Acceptable Use Agreement and has received, or will receive, safe online education to help them understand the importance of safe use of digital technology, both in and out of school
- I understand that the School will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the School cannot ultimately be held responsible for the nature and content of materials accessed on the Internet
- I will encourage my child to adopt safe use of the Internet and digital technologies at home and will inform the School if I have concerns over my child’s online safety

SCHOOL POLICY

Digital technologies have become integral to the lives of pupils/students, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Pupils/students should have an entitlement to safe internet access at all times.

THIS ACCEPTABLE USE POLICY IS INTENDED TO ENSURE:

- That pupils/students will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk

The School will ensure that pupils/students will have good access to digital technologies to enhance learning and will in turn expect the pupils/students to agree to be responsible users.

Name of pupil/student:

Class: ________________________________

Signed: ________________________________

Date: ________________________________

Parent/carer countersignature:

I agree to the guidelines set out in the Pupil/Student Acceptable Use Policy & agree to adhere to the guidelines set out in this policy.

Pupil/student Name: ________________________________

Parent/carer Name: ________________________________

Date: ________________________________

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.