Belonging, Believing; Together Succeeding

Policy: Acceptable User Policy

Date Reviewed by Staff:	**18/04/2022**
Date Reviewed by Education Committee:	**26/04/2022**
Next Review Date: (3 years unless otherwise advised)	**April 2025**

Barrington Church of England Primary School

Acceptable User Policy

Our Vision

Our vision as a Church of England primary school, deeply rooted in a strong Christian tradition, is to develop happy, young people with enquiring minds, a lifelong love of learning, respect for themselves, others and the environment so that they will have the skills, resilience and adaptability to thrive in a rapidly changing world.

Acceptable user statement

The school's policy is that no adult or child is allowed to use school computers without having signed an **acceptable user statement** (see Appendices 1 and 2 for statements). Visiting pre-school pupils will be covered by the responsible adult accompanying them having signed a statement on their behalf.

Remote access

Our school provides remote access facilities for staff using G-suite and storage via the cloud. This is managed by the ICT coordinator and Head. It is maintained securely by the LA ICT service.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

Protection from cyber attacks

Please see the glossary (appendix 3) to help you understand cyber security terminology.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure

Internet access

The school wireless internet connection is secured. We use a filtering system managed and maintained by the LA ICT service. Only visitors who need access to the school's wifi in order to fulfil the purpose of their visit will be given access on the authorization of the Head teacher.

Personal social media accounts

School staff should not accept friend requests from pupils on social media.

Related policies

This policy should be read alongside the school's policies on:

- E-safety
- Data protection
- Safeguarding
- Whistle blowing
- Behaviour
- Remote learning

Appendix 1: Pupils' acceptable user agreement

- I will only use the school's ICT equipment for schoolwork, and homework including google classroom. If I want to use the school's equipment for anything else I will ask permission first.
- I will only use MY user logins and passwords.
- I will not share my password with anyone. I will tell my teacher if I think someone else knows my password.
- I will never give out personal details e.g. photograph, address, full name or telephone number. If I have to use an online name, I will make one up.
- I will only use the internet with an adult present.
- I will make sure that all my communication is responsible, polite and appropriate.
- I will not deliberately look for, save or send anything that could be unpleasant or upsetting. If I see anything that makes me feel uncomfortable, I will always tell an adult.
- I will only look at or delete my own files.
- I will ask for permission before opening an email or an attachment from someone I do not know.
- I will only download software, pictures etc with an adult's permission.
- I understand that I must not bring software or disks into school without permission.
- I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.
- I understand that the school may check my files, emails etc. and the Internet sites I visit.
- I will never arrange to meet someone I have only previously met online. It could be dangerous.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

Name ……

Signed (child):…… (Years 1-6)*

Signed (parent/guardian): ……..
***Child's signature not required for children in Reception**

Appendix 2: Adults' acceptable user agreement

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
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.

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like 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	Programs 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 executives.