Acceptable Use Policy for Staff and Volunteers

Approved by:	Headteacher
Last reviewed:	July 2026
Next review due by:	September 2027

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications 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
- That staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

[UPDATED] For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- [NEW] I will use Multi-Factor Authentication (MFA) where required to access school systems and will never approve an MFA prompt or notification that I did not personally trigger
- [NEW] I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person

- This agreement covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for purposes such as observing what an individual is doing, taking action to prevent a crime, and using images of individuals that could affect their privacy
- The surveillance system is used to:
    - Maintain a safe environment
    - Ensure the welfare of pupils, staff and visitors
    - Deter criminal acts against persons and property.
    - Assist the police in identifying persons who have committed an offence.
    - Serve as a deterrent for violent behaviour and damage to the school.
- The school may also process biometric data, such as fingerprint recognition, facial recognition (FRT), or iris recognition, for unique identification. This includes using cameras to capture images and facial recognition technology software to produce a biometric template. FRT will be justifiable, proportionate, and able to address specific needs
- [NEW] The school will obtain explicit, informed consent before processing any staff biometric data. Staff have the right to opt-out or withdraw consent at any time without prejudice, and alternative access methods will be provided.
- [UPDATED] Any use of video conferencing technology will be fair and transparent, with participants informed of its purpose, and recording and publication of any video requiring consent and not being used outside of the intended purpose. When using video conferencing technology, check the background is plain and acceptable as if in a classroom or office (a bedroom background is not acceptable) or use a neutral background/blurred. Professional dress codes, if teaching or meeting from home must be maintained.
- I will be professional in my communications and actions when using school systems
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured
- I will only use social networking sites in school in accordance with the school's policies
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I were using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others
- [UPDATED] I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials. This includes using personal VPNs on personal devices while connected to school Wi-Fi or using unauthorised VPNs on school laptops
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage
- I understand that data protection policy requires that any staff or learner data to which I have access, including data from surveillance and CCTV systems, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority. Access to the surveillance system, software and data is strictly limited to authorised operators, and is password protected, and where appropriate, encrypted. The school's authorised CCTV system operators include James Andriot (headteacher), Aaron Armstrong (ICT Network Manager), Scott Keenan (Site Manager), and the Pastoral Support Department. The main control facility is kept secure and locked when not in use. The ability to produce copies of information is limited to appropriate staff. Any unnecessary footage captured is securely deleted. Visual display monitors are located in the ICT Office, Site Managers Office, Pastoral Office and the Headteacher's office. All surveillance footage will be kept for one month for security purposes; the headteacher and the data controller are responsible for keeping the records secure and allowing access

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

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work. Where work is protected by copyright, I will not download or distribute copies (including music and videos)
- [NEW] I will not input any personal, confidential, or sensitive data relating to pupils, staff, or the school into public Generative AI tools (e.g., AI chatbots or grading assistants). Any use of AI tools for educational or administrative purposes must comply with the school's Data Protection and AI Usage guidelines.

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: _____

Signed: _____

Date: _____