ICT Acceptable Use Policy and Agreement (Staff)

Responsibility:	HR Manager
Ratified By:	Governing Body
Date Reviewed:	October 2024
Next Review Date:	October 2026

Contents

Staff ICT Acceptable Use Policy and Agreement

1.0 School Policy

1.1 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 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 internet access at all times.

1.2 This Acceptable Use Policy is intended to ensure:

- That staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That the schools' ICT 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 ICT in their everyday work. The school will try to ensure that staff will have good access to ICT to enhance their work, to enhance learning opportunities for our young people and will, in return, expect staff to agree to be responsible users.

2.0 Acceptable Use Policy Agreement

All staff at the School are expected to use ICT systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the ICT systems and other users. All staff should recognise the value of the use of ICT for enhancing learning and should ensure that students receive opportunities to gain from the use of ICT. All staff have a responsibility for students in their care on the safe use of ICT and e-safety.

Safety for my professional and personal welfare:

- The School monitors the use of the ICT systems, email and other digital communications in order to protect the user. Any monitoring is carried out in line with Investigatory Powers Act 2016, Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 and the UK GDPR legislation and ICO monitoring guidance.
- The rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, tablets, etc.) when out of school.
- The school ICT systems are primarily intended for educational use.
- Staff should not disclose their username or password to anyone else, nor use any other person's username and password.
- Staff shall immediately report any illegal, inappropriate or harmful material or incident, they become aware of, to a member of the Senior Leadership team.

Staff are expected to be professional in their communications and actions when using school ICT systems:

- Staff shall not access, copy, remove or otherwise alter any other user's files, without their express permission.
- Staff will communicate with others in a professional manner, which will not include aggressive or inappropriate language and it is understood that others may have different opinions.
- Staff will ensure that they never use electronic communication as a means to bully or harass any members of the School community

- Staff will take great care when deciding the appropriateness of photos/videos for the students they are teaching
- Staff will ensure that when they take and / or publish images of others they will do so with their permission and in accordance with the school's policy on the use of digital / video images. They will only use my personal equipment to record these images temporarily, if the school's policies expressly permit them to do so and if the equipment is password protected/ pin coded. Images of children obtained through the school must never be retained on personal devices, after the images have been transferred onto school equipment/systems. Staff will not use personal mobile phones or other electronic equipment to photograph or video pupils unless parents have given their prior permission. Staff members will not video or photograph other staff without their individual permission
- Staff will only use chat and social networking sites in school in accordance with the School's policies and guidance listed at the end of this policy.
- Staff will reject invitations / requests from students to partake in social forums (such as Facebook, Instagram, WhatsApp and Blogging sites), instant messaging and webcams. Equally they will not make requests to students for them to join any of the above.
- Staff should only use their personal mobile phone during non-contact time for incoming/outgoing calls. It will be kept on silent mode during assemblies / lessons except for staff that have specific responsibilities that need to be contactable.
- Staff will not engage in any on-line activity that may compromise their professional responsibilities or bring the school into disrepute.
- Staff will only communicate with young people and parents / carers using official school systems. They will not give out personal details such as home / mobile number, personal email address; log in details to pupils, unless the need to do so is agreed with senior management in advance. Any such communication will be professional in tone and manner.
- If the data on any device is breached, staff will report it to the Senior Leadership Team with the Data Protection Link in the first instance, who may subsequently share with our Data Protection Officer.

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

- Where staff are expressly permitted to use their personal equipment to access the school's emails or systems (such as through an iPad, tablet, laptop, personal computer or mobile phone), they will ensure the security of that data by following the school's policies, guidance and security guides listed at the end of this policy. Staff will also follow any additional rules set by the school about such use.
- It is understood that personal information relating to pupils/students or staff cannot be stored on any personal equipment, unless expressly permitted circumstances. In such cases, the personal equipment must be encrypted or otherwise suitably protected with a pin code, password, thumb print etc.
- Staff may not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- Staff should understand the importance of ensuring their work is saved to the correct locations on school systems and 3rd party services.
- Staff will not upload, download or access any materials from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a rule, viewing a web page will be a breach of this agreement if:
- Any person (whether intended to view the webpage or not) might be offended by its contents; or
- The fact that the School's software has accessed the webpage or file might be a source of embarrassment if made public.
- They will not try to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

- Staff will not (unless they have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- Staff will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will they try to alter computer settings, unless this is allowed in school policies.
- Staff will not disable or cause any damage to school equipment, or the equipment belonging to others.
- Staff will only transport, share or retain personal information obtained through the school, as outlined in the school's Data Protection Policy and training, and will take all reasonable steps to ensure that information is kept secure. Where personal data is transferred outside the secure school network, it must be encrypted.
- Staff will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in a professional capacity or for school sanctioned personal use:

- Staff will ensure that permission has been given to use the original work of others in their own work.
- It is the staff member's responsibility to understand and comply with current copyright legislation.

It is understood that staff are responsible for their actions in and out of school:

- This Acceptable Use Policy applies not only to staff work and use of school ICT equipment in school, but also applies to their use of school ICT systems and equipment out of school, and the use of personal equipment in school or in situations related to their employment by the school.
- If a staff member fails to comply with this Acceptable Use Policy Agreement, they could be subject to disciplinary action (up to and including dismissal) and in the event of illegal activities, the involvement of the police.

3.0 Declaration

I have read and understand the Staff ICT Acceptable Use Policy and agree to use the school ICT systems (both in and out of school) and my own devices (where permitted to do so) within these guidelines.

Staff Name	
Signed	
Date	

4.0 Related Policies and Guidance:

- Safeguarding and Child Protection Policy
- Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings
- Keeping Children Safe in Education
- Guidance for schools and other establishments on the use of images
- Data Protection: A toolkit for schools, DfE
- Mobile Phone Policy
- Safer Care Code of Conduct Policy
- Information Security Policy