Staff Acceptable Use of IT Agreement

September 2026

Version	4.1
Author Initials	SW (ZW/TD)
Review Date	October 2027

Staff Acceptable Use of IT Policy Agreement

Policy Context
This Acceptable Use of IT Agreement for staff is intended to ensure that:

- Staff are responsible users and stay safe while using technologies
- School IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk from the use of IT in their everyday work and work to ensure that young people in their care are safe users.

Acceptable Use of IT Policy Agreement
I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems, other users and pupils.

Keeping Safe

- The official school email service may be regarded as safe and secure. Therefore, I know that I must only use the school email service to communicate with others.
- I know that the school can monitor my use of the school IT systems and communications.
- I know that I may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- I will comply with Education South West's password and authentication requirements, including the use of Multi-Factor Authentication (MFA) where required.
- I will only use my own user name and password which I will choose carefully so they cannot be guessed easily. I will not allow other users to access the systems using my log on details.
- I will not write my password down.
- I will ensure that my computer/laptop is not left unlocked whilst unattended and I will lock my screen (shortcut – windows button+L or Ctrl+Alt+Delete).
- I will not engage in any on-line activity that may compromise my professional responsibilities or compromise the reputation of the school or its members.
- I understand that where personal/sensitive data is transferred outside the secure school network I will ensure I use encryption and secure password protected devices.
- For this, I will ensure I use Office 365 Encrypt for sensitive personal data that I email to people/organisations outside of Education South West.
- I will ensure I use encrypted portable hard drives only and only use them if essential.
- I will use approved Education South West storage locations, such as OneDrive, Teams and designated network storage, as the location for storing files.
- I will only use my personal IT in school for permissible activities and I will follow the rules set out in this agreement.
- I will only connect personal IT to the school network using the ESWBYOD wireless network
- Under no circumstances will I allow pupils access to computers/laptops under staff logins

- I will ensure that any emails or files kept on my home devices, including my mobile phone, will be wiped/deleted (including email mailboxes) before I leave employment or if I no longer own the device.
- I will not download or back up files that contain personal information (i.e. any information with at least first name, last name or any other two identifiers) to my own personal devices/personal computers at home.
- I understand that I must immediately report, to the Safeguarding Officer or SLT – in accordance with the school policy - the receipt of any email that makes me feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Promoting Safe Use by Learners

- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- I understand that I need to have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- I will model safe use of technologies and the internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- In lessons where internet use is pre-planned, I will ensure that pupils are guided to sites checked as suitable for their use.
- I will take immediate action in line with school policy if an issue arises in school that might compromise learner, user or school safety or if a child reports any concerns.
- I will monitor learner behaviour online when using technology and deal with any issues that arise.
- I understand my role in ensuring pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Research and Recreation

- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will be vigilant with my personal use of school IT equipment.

Communicating and Sharing

- I am aware that any communication could be made public as part of a Data Protection Subject Access Request and I will ensure professionalism at all times and will not use language or phrases that I am not prepared to be made public.
- I will communicate, for all school related business, using work related/official school e-mail accounts.
- Digital communications with pupils (email / Microsoft Teams / voice) should be on a professional level and only carried out using official school systems.
- I will not use IM / social networking sites to communicate with pupils.
- I will not use IM / social networking to communicate with parents about school business.
- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will ensure that I have permission to use the original work of others in my own work and will credit them if I use it. Where work is protected by copyright, I will not download or distribute copies (including music and videos).

- I understand that staff are allowed to take digital / video images to support educational aims, but those images should only be taken on school equipment.
- Therefore, I will not use my personal mobile phone to take photos of children.
- I will only take images or video of pupils/staff where it relates to agreed learning and teaching activities and will ensure I have parent/staff permission before I take them.
- If these are to be published online or in the media I will ensure that parental / staff permission allows this by checking against GDPR compliant permissions as obtained by the school.
- Where these images are published (e.g. on the school website) I will ensure it is not possible to identify the people who are featured by name or other personal information.
- I will not use my personal equipment to record images / video of pupils unless the content relates directly to an immediate family member.
- I will not keep images and videos of pupils stored on my personal equipment unless the content relates directly to an immediate family member.

Problems

- I will immediately report any suspected misuse, illegal, inappropriate or harmful material or incident I become aware of to the Safeguarding Officer for investigation / action / sanction
- If I believe a young person may be at risk, I will follow the child protection procedures.
- Any incidents will then immediately be reported to the ESW IT Director, and the ESW Data Protection Officer if there has been a personal data breach.
- If I believe a young person may be being bullied, I will follow the anti-bullying procedures.
- I will not download, install or store applications or software on any ESW computer without obtaining permission from the ESW IT Director.
- Where a digital tool requires the creation of user accounts or the processing of personal data, I will ensure that it has been recorded with the ESW Compliance Team.
- I understand that computer settings are locked down for a reason and I will not try to alter these settings or circumnavigate restrictions.
- Any filtering issues should be reported immediately to the ESW IT Services Team.
- I will immediately report any damage or faults involving equipment or software, however this may have happened to the ESW IT Services Team.
- I will 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.
- I will not open emails from unknown or suspicions sources and I will ensure I contact IT Services regarding any suspicious emails, links in emails, or attachments.

Personal Devices and Access to Trust Systems

- If I use any personal device to access Education South West systems, services, data, networks, Wi-Fi, email, Microsoft 365, or other organisational resources, I understand that Education South West may require me to provide information or evidence relating to the security of that device.
- Such evidence may include screenshots, system information, configuration details, software version information, or other reasonable proof requested by Education South West.

- I will cooperate with reasonable requests for information or evidence relating to the security of any personal device used to access Education South West systems, services or information.
- I understand that these checks may be required to support cyber security, safeguarding, data protection, insurance, audit or regulatory requirements, including Cyber Essentials Plus assessments.
- I understand that failure to provide requested information, or concerns arising from the information provided, may result in access to Education South West systems, services, networks or data being restricted, suspended or removed.

AI (Artificial Intelligence)

- I will not enter, upload, share, or process personal data, special category data, confidential information, safeguarding information, commercially sensitive information, or any other information that I am not authorised to disclose within an AI tool unless explicitly authorised by Education South West.
- I will comply with all Education South West policies relating to data protection, information security, safeguarding, confidentiality, and acceptable use when using AI technologies.
    - Data Protection Policy
    - Information Security Policy
    - GDPR Privacy Notice
- I will not upload or submit pupils' work, assessment data, staff information, safeguarding records, or other school business information to an AI tool unless its use has been approved by Education South West and any required permissions have been obtained.
- I understand that AI-generated content may be inaccurate, incomplete, biased, misleading, or out of date. I will exercise professional judgement and verify the accuracy, appropriateness, and suitability of any AI-generated content before using, sharing, or relying upon it.
- I understand that AI-generated content must not be used as the sole basis for safeguarding, behaviour, educational, employment, disciplinary, financial or other significant decisions affecting individuals.
- I remain responsible for any work, decisions, communications, or content produced with the assistance of AI and will not rely solely on AI-generated outputs.
- I will not use AI to create, access, share, or distribute material that is inappropriate, unlawful, discriminatory, harmful, misleading, or contrary to Education South West policies.
- Where AI-assisted content is used in educational, operational, or administrative activities, I will ensure that its use is transparent and consistent with Education South West's legal, ethical, safeguarding, and professional obligations.
- I will seek guidance from the ESW IT Team, Data Protection Lead, or appropriate senior leader if I am unsure whether a proposed use of AI is permitted.

I understand that these rules are in place to enable me to use IT safely and securely and that failure to comply with them may result in disciplinary action.
I agree to comply with this Acceptable Use of IT Agreement whenever:

- I use Education South West or school IT systems, whether on-site, at home, or from any other location.
- I use my own IT equipment, including mobile devices, to access Education South West or school systems, services, networks, applications, or data.
- I access Education South West systems, services, applications, networks, or data using any device.

I understand that Education South West may monitor, audit, and review the use of its systems, applications, accounts, networks, and data to ensure compliance with legal, safeguarding, operational, and cyber security requirements.

Employee Name	
Signed	
Date	