Staff & Volunteers Acceptable Use Agreement
2026–2027

Purpose of this agreement

This Acceptable Use Agreement sets out the expectations for staff and volunteers when using the school's IT systems, devices, online services and digital communications. It is intended to protect children, staff, school information and IT systems, and to support the safe, responsible and professional use of technology.

At Sir Francis Hill Primary School, digital technology is used to enhance teaching, learning and the effective running of the school. Staff and volunteers have a duty to model safe and responsible use, maintain professional boundaries and help children develop the knowledge and skills they need to use technology safely.

General responsibilities

- I will use school IT systems, devices and online services responsibly, professionally and in accordance with school policies.
- I understand that school IT systems are primarily provided for educational and professional use. Any limited personal use must comply with school rules and must not interfere with my work or the operation of school systems.
- I will treat others with respect in all digital communications and will not create, access, store, share or transmit material that is unlawful, inappropriate, discriminatory, harmful, offensive or likely to bring the school into disrepute.
- I will not attempt to bypass filtering, monitoring or security controls, gain unauthorised access to accounts or systems, introduce malicious software, or install software without authorisation.
- I will immediately report illegal, inappropriate or harmful material, online-safety incidents or safeguarding concerns to Designated Safeguarding Lead (DSL) or Deputy Designated Safeguarding Lead (DDSL), the Data Protection Officer (DPO) or a member of the Core Leadership Team, as appropriate.

Accounts, passwords and device security

- I will keep my username, password and authentication details secure and will not share passwords, verification codes or multi-factor authentication (MFA) approvals with anyone.
- I will not approve an MFA request that I did not initiate and will report unexpected authentication prompts or suspected account compromise.
- I will not use another person's account or allow another person, including a pupil, to use a device while it is signed in under my staff account.
- I will lock or secure a device whenever I leave it unattended and will take reasonable steps to prevent unauthorised access to confidential information.
- I will promptly report lost, stolen, damaged or faulty school equipment, or any suspected security incident.
- I will exercise caution with links, QR codes and email attachments and will not open unexpected or suspicious content, even when a message appears to come from a known sender.
- I understand that use of school devices, networks, email systems and online services may be logged, monitored, filtered and reviewed by authorised personnel for safeguarding, security, legal and operational purposes. Users should not expect complete privacy when using school-owned systems.
- When working remotely, I will take reasonable precautions to protect school information from being viewed, overheard or accessed by unauthorised persons.

Filtering and monitoring systems

- I understand that the school operates filtering and monitoring systems designed to safeguard children and protect school systems and I will not attempt to interfere with their operation.

Data protection, storage and cloud services

- I will keep staff and pupil information private and confidential and will only access, use or disclose it where there is a legitimate professional need and in accordance with the school's Data Protection Policy.
- I will only store, process or share school information using systems and services approved by the school.

- I will not transfer school information to personal email accounts, personal cloud-storage services, personal messaging services or other unauthorised platforms.
- I will use the school's approved cloud-based storage systems rather than personal memory sticks or other removable storage unless specific permission has been given.
- I understand that authorised school personnel may access school systems, accounts and information where this is necessary for safeguarding, security, administration, legal compliance or the effective running of the school.

Professional communication and social media

- I will communicate with pupils and parents/carers only through official school-approved systems and will ensure that all communication is professional in tone and content.
- I will not use personal social-media or messaging applications including WhatsApp, Facebook Messenger, Snapchat or similar services, to communicate privately with pupils.
- I will maintain appropriate professional boundaries with parents/carers and former pupils when using social media and messaging services.
- I will take reasonable steps to secure my personal social-media accounts and will not post comments, images or information that compromise pupil or staff confidentiality, safeguarding, professional standards or the reputation of the school.
- I will not access, copy, remove or alter another user's files without authorisation.

Photographs, video and audio

- I will check the parental consent information held within the school's management information system before taking or publishing photographs or video of pupils.
- I will only use school-authorised equipment to take photographs, video or audio of pupils and will not use a personal mobile phone or other personal device for this purpose.
- Where school information is accessed through a personal device, I will ensure that the device is protected by a password, PIN, biometric authentication or equivalent security measure.
- I will only take and use images or recordings for legitimate school purposes and in accordance with the school's Safeguarding and Child Protection Policy and any relevant media/photography guidance.
- Where images are published, I will follow the school's rules about identification and will not include unnecessary personal information.
- I will ensure images are appropriate and will take particular care in higher-risk contexts such as swimming, changing activities, performances and drama.
- I will encourage pupils to speak to a trusted adult if they are worried or uncomfortable about an image or recording.
- I will not allow external photographers unsupervised access to pupils.

Artificial intelligence (AI) and generative AI

- I will only use AI tools for school purposes where their use is appropriate and consistent with school policies, safeguarding requirements and data-protection obligations.
- I will not enter personal, confidential, sensitive or identifiable information about pupils, families, staff or the school into publicly available or unapproved AI systems.
- I remain professionally responsible for any AI-generated material I use. I will check it for accuracy, bias, suitability, copyright concerns and age appropriateness before using or sharing it.
- I will not use AI to create, alter or share content that is deceptive, harmful, discriminatory, inappropriate or likely to compromise safeguarding or professional standards.
- Where AI is used with pupils, I will model safe, responsible and age-appropriate use and follow the school's agreed approach to AI and online safety.
- Where AI-generated content contributes significantly to professional work, assessment, communication or reports, I will ensure appropriate professional oversight and verify the information before use.

Use of personal devices and school systems

- When using a personal device on school premises or for school-related activity, I will follow this agreement and all relevant school policies.
- I will not connect unauthorised devices, storage media or services to school systems where doing so could create a security or data-protection risk.
- I understand that this agreement applies to my use of school IT systems and equipment both on and off the school premises, and to my use of personal equipment when carrying out school-related activity.

- I will not make unusually large downloads or uploads, disable equipment, or undertake activity that could unnecessarily disrupt school systems or technical support.

Copyright and appropriate use

- I will respect copyright, licensing and intellectual-property rights and will obtain permission or use appropriately licensed material where required.
- I will not unlawfully download, copy or distribute copyrighted material, including music, video, software or other digital content.

Reporting concerns and incidents

- I will report safeguarding, online-safety, data-protection and cyber-security concerns immediately using the school's agreed procedures and will not attempt to investigate or resolve them independently. This includes suspected phishing, accidental disclosure of information, lost or stolen devices, inappropriate online contact, harmful content, security weaknesses and any situation where a pupil or member of staff may be at risk.

Responsibility and compliance

- I understand that I am responsible for my actions when using school technology and when using personal technology in connection with my role.
- I understand that failure to comply with this Acceptable Use Agreement may result in action under the school's relevant procedures. Serious or illegal activity may also be referred to the Local Authority, police or other appropriate authority.

Staff & Volunteer Agreement

I have read and understood this Acceptable Use Agreement and agree to use the school's IT systems, devices, online services and my own devices, where used for school-related activity, in accordance with these expectations. I understand that this agreement should be read alongside the school's Online Safety Policy, Safeguarding and Child Protection Policy, Staff Code of Conduct and Data Protection Policy.

Name: **Role:**

Signature: **Date:**

Volunteer / Staff (delete as appropriate):

(Staff and Volunteer agreement may be gained via CPOMS if an allocated user).

Key contacts

Designated Safeguarding Lead (DSL)	Miss Danni Lacey (SENDCo) Mrs Cal Smith (Safeguarding & Welfare)
Deputy Designated Safeguarding Leads (DDSL)	Mrs Vicky Cook (EYFS Lead, SENDCo) Mrs Sammy Robinson (Parent Support Advisor) Mrs Karen Revill (Welfare and Attendance)
Data Protection Officer (DPO)	SBM Services - Data Protection Officer Support.

Agreement written: September 2026