



Staff and Volunteers Acceptable Use Agreement 2025-2026

Aim of the Staff and Volunteers Acceptable Use Agreement

The aim of this Acceptable Use Agreement is to ensure that children will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet and email use and access is considered a school resource and privilege. Therefore, if the school's Acceptable Use Agreement is not adhered to this privilege will be withdrawn and appropriate sanctions imposed.

At Sir Francis Hill Primary School, we use IT, the internet and mobile technology to enhance the children's learning experiences and support their educational development. We aim to help children develop and build their technological skills for the future and value the use of IT in school as an educational tool. Parents / carers are required to give permission for their child to use mobile devices and access the internet as part of the curriculum when they enter the school. The school will ensure safe internet provision through its internet provider and will monitor the pupils' use of the internet and address issues of pupils trying to access an unauthorised site.

We can transform and enhance education and help children to fulfil their potential and raise standards with IT. However, we also have a duty of care and must ensure that we are able to safeguard children and staff, so it is also important that children learn how to be safe when they are using new technologies. Whilst filtering and blocking is part of our policy, we believe a more sustainable approach is required. We will equip the children with the skills and knowledge they need to use the internet safely and responsibly, managing the risks wherever and whenever they go online; to promote safe and responsible behaviours in using technology both at school and in the home and beyond.

Risks

Staff and pupils are at potential risk from the use of the internet. The risk is often determined by behaviours rather than the technology itself.

- Commercial
- Aggressive
- Sexual
- Values
- Content (child as recipient)
- Adverts, spam, sponsorship
- Personal Information
- Violent/hateful content
- Pornographic
- AI
- Unwelcome sexual content
- Contact (child as participant)
- Tracking
- Harvesting personal information
- Being bullied, harassed or stalked
- Meeting strangers
- Being groomed
- Self-harm
- Unwelcome persuasions
- Illegal downloading
- Hacking
- Gambling
- Financial scams
- Terrorism

- Bullying or harassing one another
- Creating inappropriate material
- Uploading inappropriate material
- Providing misleading information

General Strategies to Reduce Risk

The school employs several strategies in order to maximise learning opportunities and reduce risks associated with the internet. These strategies are as follows:

- All computing equipment is maintained and supported by an external technical support team.
- A filtering system called Securly, is used to minimise the risk of exposure to inappropriate material.
- E-Safety and the use of IT equipment is monitored by the Senior Leadership Team and Safeguarding Team.
- Children will be regularly taught about and reminded about internet safety and e-safety will be promoted through all digital learning and the computing curriculum.
- The use of personal memory sticks or other digital storage media in school for children requires a teacher's permission and for staff is rarely needed due to the cloud-based storage systems in place.
- Children and staff will always treat others with respect and will not undertake any actions that may bring the school into disrepute.

Use of Facilities

It is not acceptable for staff and children to:

- Attempt to introduce a virus or malicious code to the school network.
- Attempt to bypass network or system security.
- Attempt to gain access to an unauthorised area or system.
- Attempt to use any form of hacking / cracking software or system.
- Access, download, create, store or transmit material that could cause annoyance or offence or anxiety to others, infringes copyright or is unlawful, brings the name of the school into disrepute.
- Engage in activities that waste technical support time and resources.

It is not acceptable for children to:

- Attempt to download, store or install software to school computers.
- Attempt to access another user's account.
- Connect any device to the network that has access to the internet via a connection not provided by the school.

This Acceptable Use Agreement is intended to ensure:

- That staff and volunteers will be responsible users, stay safe and keep others (particularly children) safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school IT 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 IT in their everyday work.
- The school will ensure that staff and, if necessary, volunteers will have good access to IT to enhance their work, to enhance learning opportunities for pupils' 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 IT systems and technology in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users, especially children. I recognise the value of the use of IT for enhancing learning and will ensure that children receive opportunities to gain from the use of IT. I will, where possible, educate the children and young people in my care in the safe use of IT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g. laptops, emails etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school IT 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.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to a Designated Safeguarding Lead, Data Protection Officer or a member of the Senior Leadership Team.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I will appreciate that others may have different opinions.
- I will ensure when using school ICT system any communications, documents, files or storage areas are accessible to the school Senior Leaders.
- 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; if I do use my personal equipment to take images, I will delete them at the earliest opportunity. Where these images are published it will not be possible to identify by full name, or other personal information, those who are featured. I will also check on our school MIS (Arbor) that the parents have given permission for their child's photo to be used)
- Should I be a member of social networking sites, I will keep my profile secure (using the highest security settings) and will avoid contact with parents, pupils and/or ex pupils related to the school. I understand that any action or comment made by myself that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a disciplinary matter.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner and will not engage with any activity that may compromise my professionalism.

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

- When I use my mobile devices (laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- 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.
- 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 not try to use any programmes or software that might allow me to bypass the filtering and security systems in place to prevent access to such materials.
- I will not (unless I 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.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that Data Protection policy requires that any staff or pupil data to which I have access, 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.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet 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).

When taking photographs of children in school, in line with the school's Child Protection & Safeguarding Policy, I will aim to:

- Check the Parental consent for photos on Arbor.
- Not take a photograph if consent is not given (using records held on Arbor to establish if permission is present)
- Only use school equipment to take photographs
- Only take photos and videos of children to celebrate achievement
- Use only the child's first name with an image

- Encourage children to tell us if they are worried about any photographs that are taken of them.
- Only use images of children in suitable clothing to reduce the risk of inappropriate use. Some activities, for example swimming and drama, present a much greater risk of potential misuse.
- Not allow photographers from outside of school unsupervised access to children

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

- I understand that this Acceptable Use Agreement applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT 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 and / or the Local Authority and in the event of illegal activities the involvement of the police.

Staff Agreement *As a member of staff at Sir Francis Hill Primary School, I have read and understand the above and agree to use the school IT 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. I understand that I will use any technology or school IT systems in line with the Safeguarding and Child Protection Policy and Data Protection Policy. Any safeguarding and data security concerns that I do have will be reported as soon as possible.*

Designated Safeguarding Lead (DSL)

Miss. Danni Lacey (DSL)
Mrs. Cal Smith (DSL)

Deputy Designated Safeguarding Lead (DDSL)

Mr Neil Fish-Clark (Assistant Head Teacher)
Mrs. Lynn Garner (Assistant Headteacher)
Mrs. Karen Revill (Welfare Officer)
Mr. Barry Dennis (Learning Mentor)

Data Protection Officer (DPO)

Mr Neil Fish-Clark (Assistant Head Teacher)



Agreement Written: September 2025