



Farsley Springbank Primary School

‘Be the best you can be.’

Online Safety policy



1. Aims

At Farsley Springbank Primary School, our approach to online safety is rooted in our core values of being Courageous, Kind and Curious. We recognise that technology plays an essential role in children’s lives and that it is our responsibility to ensure pupils are supported to use it safely, responsibly and positively.

Our school aims to:

- **Create a safe and supportive online environment** where pupils, staff, volunteers and governors are protected from harm and feel confident to report concerns, showing courage when something does not feel right
- **Promote kindness and respect in all online interactions**, helping pupils understand the impact of their digital behaviour on others and fostering positive, inclusive and responsible online communities
- **Encourage curiosity in a safe and informed way**, empowering pupils to explore digital technology, information and online opportunities thoughtfully, critically and with appropriate safeguards in place
- **Identify and support pupils who may be more vulnerable to online risks**, ensuring our approach is inclusive and responsive to individual needs, including those with SEND or additional safeguarding vulnerabilities
- **Provide clear education and guidance** for pupils, staff and families so that everyone understands how to use technology safely, responsibly and in line with school expectations
- **Establish clear systems for prevention, reporting and response**, enabling concerns to be identified early and addressed proportionately, consistently and effectively
- **Equip pupils with the knowledge and skills to make safe choices online**, both in and beyond school, helping them to become confident, responsible digital citizens

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-

consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

This policy also reflects the DfE's Filtering and Monitoring Standards (2023), which schools are required to meet and evidence annually

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

This policy also reflects the DfE's filtering and monitoring standards and guidance (2023) on meeting digital and technology standards for schools.

3. Roles and responsibilities

3.1 The governing body

The governing board has overall responsibility for ensuring that this online safety policy is effective and compliant with statutory guidance. It holds the headteacher to account for its implementation.

The governing board will:

- Ensure that online safety is treated as a key safeguarding priority and is embedded within the school's wider safeguarding culture
- Ensure that appropriate filtering and monitoring systems are in place on all school devices and networks, and that these systems are reviewed for effectiveness at least annually
- Review the DfE filtering and monitoring standards and ensure the school meets these expectations.

- Ensure that roles and responsibilities for filtering and monitoring are clearly defined and understood
- Receive regular reports from the designated safeguarding lead (DSL) on online safety incidents, trends and concerns
- Ensure all staff, governors and relevant volunteers receive appropriate online safety training as part of safeguarding training and ongoing updates
- Ensure pupils are taught how to keep themselves and others safe online through the curriculum
- Ensure that online safety arrangements are inclusive and adapted where necessary to support vulnerable pupils and those with SEND

All governors will:

- Read and understand this policy
- Agree to and adhere to the staff acceptable use agreement
- Ensure safeguarding, including online safety, is considered when making strategic decisions

3.2 The Headteacher

The headteacher is responsible for ensuring that this policy is implemented consistently and effectively across the school.

The headteacher will:

- Ensure all staff understand their responsibilities in relation to online safety
- Support the DSL in fulfilling their online safety role
- Ensure appropriate resources, training and systems are in place to support online safety
- Ensure that concerns are responded to promptly and proportionately

3.3 The designated safeguarding lead (DSL)

The DSL takes **lead responsibility for online safety** within the school. Details of the DSL and any deputies are outlined in the child protection and safeguarding policy.

The DSL is responsible for:

- Leading on the development, implementation and review of this online safety policy
- Working with the headteacher and governing board to ensure online safety arrangements remain effective and up to date
- Having a clear understanding of the school's filtering and monitoring systems, including how safeguarding alerts are generated and responded to
- Working closely with the ICT provider to ensure systems support safeguarding needs
- Responding to concerns identified through filtering and monitoring systems
- Managing and recording online safety incidents in line with safeguarding procedures
- Ensuring incidents of cyberbullying are recorded and addressed in line with the behaviour policy
- Providing advice and support to staff when online safety concerns arise

- Liaising with external agencies where necessary, including the local authority and police
- Delivering and coordinating online safety training and updates for staff and governors
- Providing regular reports to the headteacher and governing board on online safety issues and trends
- Undertaking an annual online safety risk assessment to reflect emerging risks and changes in technology

This list is not intended to be exhaustive.

3.4 The ICT provider / network manager

The school's ICT provider, **Dataable**, is responsible for the **technical operation** of the school's ICT systems.

This includes:

- Implementing and maintaining appropriate filtering and monitoring systems on school devices and networks
- Ensuring systems are reviewed and updated regularly to protect pupils from harmful or inappropriate content, including extremist material
- Maintaining the security of the school's ICT systems, including protection against viruses and malware
- Monitoring system performance and security on a regular basis
- Blocking access to unsafe or inappropriate websites and downloads
- Supporting the DSL and headteacher in responding to online safety incidents where required

Overall safeguarding accountability remains with the DSL and senior leadership.

3.5 All staff and volunteers

All staff, including agency staff, contractors and volunteers, share responsibility for safeguarding pupils online.

They are responsible for:

- Reading, understanding and following this policy
- Implementing online safety procedures consistently
- Adhering to the staff acceptable use agreement
- Supporting pupils to follow the pupil acceptable use agreements
- Being aware of how to report concerns related to filtering and monitoring systems
- Reporting any online safety concerns or incidents to the DSL promptly
- Responding appropriately to concerns about online abuse, including peer-on-peer abuse and sexual harassment, maintaining an attitude of *"it could happen here"*

3.6 Parents and carers

Parents and carers are expected to:

- Support the school in promoting online safety
- Ensure their child understands and follows the pupil acceptable use agreement
- Raise any concerns about online safety with the school promptly

Parents and carers can access further guidance from:

- UK Safer Internet Centre
- Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be:

- Made aware of this policy where relevant
- Expected to follow the school's acceptable use arrangements
- Asked to sign an acceptable use agreement where appropriate

4. Educating pupils about online safety

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For

example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this

- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, on our website and may contact parents via app message if applicable. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyberbullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one

person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and anti-bullying policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their pupils.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and Anti-Bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Farsley Springbank recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. Farsley Springbank will treat any use of AI to bully pupils very seriously, in line with our Anti-bullying policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

7. Acceptable use of the internet in school

7.1 Internet use

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. Staff will always use a child friendly safe search engine when accessing the web with pupils.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day. On arrival into the school playground children hand their phones in and they are then stored in the school office until the end of the school day (or after an after school club) when they can be collected.

Any wearable technology with internet capability (e.g. smartwatches) will be treated in line with the mobile phone policy.

Any breach of this is subject to the conditions of behaviour policy.

Exceptions where pupils may need their mobile phone in school, such as monitoring for diabetes will be agreed in advance with the Headteacher.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol) and changing passwords regularly.
- Activating 2-step authentication on their school Google drive, ensuring personal Google accounts are not linked.
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software (DataCable's responsibility)
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager (DataCable).

10. Staff using personal devices in school

The use of any personal equipment in schools should always be with the prior permission of senior management in order to comply with health and safety regulations and members of staff should take care to comply with the staff acceptable use policy and Safer Working Practices guidance.

All staff personal devices must be connected to the school wifi whilst on the premises so that the school filtering system is in use.

Personal equipment capable of recording images, moving images or sounds and those used for accessing the internet such as iPads, mobile phones, cameras, video cameras and laptops should not be used in work time outside of the staffroom without the prior permission of senior management. Staff must never use personal devices to take photographs or videos of children, there are school camera and iPads for this purpose. Staff should only use their mobile phones for personal use in the staffroom over break/lunchtimes and never in front of any pupils. Staff should not have their phones available at any time in their classrooms or around their pupils. Any personal equipment of this sort should be stored in a secure location within the classroom in case of evacuation.

The only exceptions to this are when staff may need to use their personal device to access two factor authentication for systems such as CPOMS. This should be done when there are

no children in the classroom and personal devices should be securely stored away straight after use. In addition to this in an invacuation situation, authorisation has been given to staff that they may need to use their mobile phones to contact other members of staff/Headteacher to report on the safety and whereabouts of all staff/pupils.

Any member of staff found to be using such personal equipment without prior authorisation may be subject to disciplinary action.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up

- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term
- have an awareness of AI tools, deepfakes, scams and influencer culture.

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding and child protection policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using our secure safeguarding software (CPOMS).

This policy will be reviewed every year by the computing lead and the DSL. At every review, the policy will be shared with the governing body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to our:

- Safeguarding and child protection policy
- Behaviour policy
- Anti-bullying policy
- Disciplinary policy
- Data protection policy
- Complaint policy and procedures
- Staff acceptable use policy – Appendix 3
- Pupil acceptable use policy – Appendix 1 and 2

Online Safety approved by the full Governing Body in February 2026

To be reviewed in February 2027

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR EYFS AND KS1 PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers and iPads) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR KS2 PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers and iPads) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carers
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Use any inappropriate language when communicating online
- Create, link to or post any material that is offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carers, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will ensure it is handed in when I arrive at school and understand that I am not allowed to use it once I have entered into the school grounds. When I collect my personal device at the end of the school day, I will not use it until I have left the school premises.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carers' agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carers):

Date:

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking the correct permissions are in place and where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- Use my personal equipment to take photographs or videos of children in school. I will only use school equipment for these purposes.
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

I will only use the school's ICT systems and access the internet in school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. An exception may be using a personal mobile to generate code for two factor authentication to access secure school systems.

Outside school, where possible I will use a work device, however, if I am accessing the school's IT systems such as Google Drive and work emails on a personal device, I will ensure I have the appropriate security measures in place and that I log out of devices so no other family members can access school systems and information.

I will take all reasonable steps to ensure that work devices and personal devices (if being used for work purposes) are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will let the designated safeguarding lead (DSL) and Headteacher know if a pupil informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I will ensure that any personal devices in school (e.g. mobile phones) are connected to the school WIFI and not on 3G/4G/5G and that personal devices are stored securely in school and only used outside teaching time when children are not present.

I understand that this Acceptable Use Policy applies not only to my work and use of school 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 Policy 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.

Signed (staff member/governor/volunteer/visitor):

Date: