Farsley Farfield Primary School

Online Safety Policy 2023

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, that empowers us to protect and educate the whole school community in its use of online technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

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.

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. Programmes of study for the Farsley Farfield curriculum can be seen in the Computing and the PSHE sections of the school's online curriculum document here.

3. Roles and responsibilities

3.1 The governing body

The governors have overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Safeguarding governors will meet with appropriate staff to discuss online safety, and monitor sample online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all

situations, and a more personalised or contextualised approach may sometimes be more suitable.

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, IT support worker and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with this policy and the school child protection policy
- Ensuring that any online safety incidents are logged on CPOMS **(Behaviour: misuse of IT/online concern)** and dealt with appropriately in line with this policy and the school's behaviour policy
- Ensuring that any incidents of cyber-bullying are logged (tagged as Behaviour: misuse of IT/online concern ***and other appropriate categories e.g. bullying, abusive behaviour)*** and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Network Manager/Technical staff

Datacable, our technical services provider, are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material **(Netsweeper and Securly)**
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly **(SOPHOS)**

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files **(SOPHOS, Netsweeper and Securly)**

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Adhering to the expectations of section 12 of Safer Working Practice relating to restrictions on communicating online with children and young people, and as regards professional behaviour online out of school

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read/understood and agreed to the terms on acceptable use of the school's IT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and be expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4 Educating pupils about online safety

Pupils will be taught about online safety ensuring coverage of:

National Curriculum computing programmes of study

Guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Farfield follows a framework of online safety from the Purple Mash Computing Scheme of Work. In Years 1-6, there is a unit of work every year, typically in the autumn term.

4.1 In **Key Stage 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

4.2 Pupils in **Key Stage 2** will be taught:

	E-Safety		
National Curriculum subject content	**Pupils should be taught to:** ● use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact		
Y3 & Y4 Objectives	**Rules** ● Follow the school's safer Internet rules ● Agree sensible e-Safety rules for the classroom ● Understand the need for rules to keep them safe online ● Know that copyright exists on most digital images, video and recorded music ● Know that cyber-bullying is unacceptable and will be sanctioned in-line with the school's anti-bullying policy	**Personal safety** ● Understand the need to develop an alias for some public online use ● Use caution when using an Internet search for images ● Know what to do if they find an unsuitable image ● Understand that personal information and passwords should be kept private ● Know that any personal information made available online may be seen and used by others ● Know how to respond if they are asked by someone for personal information ● Know how to report an incident of cyber-bullying ● Choose a secure password for age-appropriate websites	**Communication** ● Identify when emails should not be opened ● Know that some attachments may not be safe ● Explain how to use email safely ● Know how to respond if they feel unsafe about the content of a message
Y5 & Y6 Objectives	**Rules** ● Follow the school's safer Internet rules ● Agree sensible e-Safety rules for the classroom	**Personal safety** ● Discuss their own personal use of the Internet and choices they make ● Discuss the importance of keeping an adult informed about what you are doing online, and how to report concerns ● Create strong passwords and manage them so that they remain strong ● Understand that online resources might have	**Communication** ● Discuss how to protect devices from virus threats ● Explore using the safe and responsible use of online communication tools such as blogs and messaging ● Select and use appropriate communication tools, with regard to e-Safety, to collaborate with others within and beyond the school

		security settings that can be used or amended to protect the user ● Understand the benefits of using a nickname for online use ● Know that it is unsafe to arrange to meet unknown people online ● Know how to report anything suspicious ● Know what to do if they discover anything malicious or inappropriate online ● Understand the potential risk of sharing personal information online	● Understand the potential risks of using Internet communication tools, such as phishing or scamming, and how to minimise these risks ● Understand that some messages might be malicious, and how to deal with them ● Understand that they should not publish other people's pictures on the Internet without permission ● Know that content published online is extremely difficult to remove ● Understand that some malicious adults may use a variety of techniques to make contact and try to get personal information

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' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Key information about online safety is included on our website: https://www.farsleyfarfield.org.uk/safeguarding-and-e-safety/

If parents 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.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the 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 consider whether the incident should be reported to the police if it involves illegal material, and will 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.

Key Stage 2 pupils have school Chromebooks that they take home and use out of school time. These can be physically searched and accounts can be remotely monitored/examined through Netsweeper, Securly and Google Vault.

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.

7. Acceptable use of the internet in school

7.1 Internet use

All pupils (Y1-6), parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT 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.

8. Pupils using mobile devices in school

Year 5/6 pupils may bring mobile devices into school, but are not permitted to use them during the school day. On arrival into the classroom, the children

hand their phones in and they are then stored in the classroom until the end of the school day when they can be collected.

Any breach of this is subject to the conditions of the 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
- 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 IT 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.

Personal equipment capable of recording images, video 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 should not use personal devices to take photographs or videos of children; there are school cameras, phones and iPads for this purpose. Staff can, however, use personal mobile phones to photograph students' work without a student in the picture.

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 be using their personal phones in work time except for explicit work purposes such as email (if a computer is not readily available) or for two factor authentication.

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 IT systems or internet, we will follow the procedures set out in our policies on Behaviour 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 IT 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 every 3 years as part of safeguarding training, as well as relevant updates as required (for example through emails and staff briefings).

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, 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

The DSL and safeguarding team 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

Behaviour and safeguarding issues related to online safety will be logged using our secure safeguarding software (CPOMS). The DSL will provide an overview report on online safety to Pupil Support Sub Committee annually.

The headteacher will receive automated alerts of blocked online pupil activity and action appropriately.

This policy will be reviewed every 3 years by the computing lead and the DSL. At every review, the policy will be shared with the governing body.

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
- Safer Working Practice
- Staff acceptable use policy – Appendix 3
- Pupil acceptable use policy – Appendix 1 and 2

Online Safety to be approved by Pupil Support committee June 2023

To be reviewed every 3 years – due June 2026

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

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR KS1 PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's IT systems (like computers and iPads) and get onto the internet in school I will: ● Only use websites that a teacher or adult has told or allowed me to use ● Tell my teacher immediately if: o I click on a website by mistake o I receive messages from people I don't know o 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 IT 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 where asked: in my Google Drive or within Purple Mash for example ● 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 IT 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 IT 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 IT 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 IT systems (typically using a Chromebook) and get onto the internet in school in lesson times, I will: ● Always use the school's IT 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/carer ● 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 in school time, unless my teacher has expressly allowed this as part of a learning activity ● Use any unkind or rude language when communicating online ● Create, use, 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/carer, or without adult supervision ● Actively seek to bypass the security settings put in place on the Chromebooks by school **If I bring a personal mobile phone or other personal electronic device (upper KS2) 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/carer's agreement: I agree that my child can use the school's IT 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 IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. I agree that my child's use of their Chromebook at home will be monitored by the Securly filtering system and, ideally, the home's own child-friendly wifi settings. If the school is alerted to concerning use of the Chromebook at home, I will be contacted.	
Signed (parent/carer):	**Date:**

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

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

Name of staff member/governor/volunteer/visitor:

When using the school's IT 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 IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

I will only use the school's IT 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 or to access a work email account or calendar.

Outside school, if I am accessing the school's IT systems such as Google Drive and work emails on a shared 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 IT 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 IT systems and internet responsibly, and ensure that pupils in my care do so too.

I will ensure that personal devices are stored securely in school and only used outside teaching time for personal use when children are not present. Mobile phones must not be in pockets when working in care suites/changing rooms.

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:**