Foxbridge Primary School

Online Safety Policy

Written: April 2025

Review: April 2026

Signed copy held centrally

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, volunteers and governors
- Deliver an effective approach to online safety which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as mobile phones)
- 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 radicalistation and extremism

Contact – being subjected to harmful online interaction with others users such as peer-to-peer pressure, commercials 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

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 (DFE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice on

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

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. The policy also takes into account the National Curriculum computing programmes of study and complies with our funding agreement and articles of association.

3. Roles and responsibilities

The Governing Body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and internet (*Appendix 1)*
- 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 often be more suitable

The headteacher

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

- work with the ICT Lead and other staff as necessary to address online safety issues or incidents
- Manage all online safety issues and incidents in line with the school child protection policy
- Ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Update and deliver staff training on online
- Liaise with other agencies and/or external services if necessary
- Provide regular reports on online safety in school to the Governing Body

The ICT lead

The ICT lead is 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

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

    - Firewall by Nasstar
    - Filtering is Netsweeper
    - Anti-virus software is Sophos
    - Monitoring software is Senso

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 ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use (appendix 2)
- Working with the headteacher to ensure that any online safety incidents are logged (see appendix 3) 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'

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the Early Years Foundation Stage (EYFS) Curriculum and National Curriculum.

In **EYFS,** pupils will be taught to

Use technology safely and understand the importance of asking permission to use electronic devices and online games

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

In **Key Stage 2**, pupils 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

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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.

Working with Parents

Foxbridge Primary School will raise parents' awareness of internet safety and the potential dangers of online social spaces in letters or other communications home, and in information via our school website. This policy will also be shared with parents.

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

Cyber-bullying

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.

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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

Mobile Devices in School

Children are encouraged not to bring mobile devices in to school. If they need to bring one into school, it will need to be left in the school office.

Staff will not use mobile phones during contact time with the children or in view of children.

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
- Making sure devices are locked when left unattended
- Only using work devices for work activities

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.

Training

All new staff members will receive safeguarding training as part of their induction. This includes 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). Through this training, 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

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

Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to read and agree to the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). 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.

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

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 behaviour policy. The incident will also be logged via CPOMS ~~in the online safety log (appendix 3)~~ 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 disciplinary procedures.

Monitoring Arrangements

The headteacher logs behaviour and safeguarding issues related to online safety (appendix 3).

This policy will be reviewed annually by the Governing Body.

Appendix 1

Acceptable Use Agreement – Staff

Note: All Internet and email activity is subject to monitoring

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking –Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment.

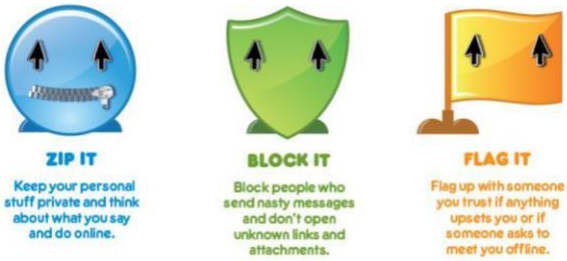
e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

NAME :

SIGNATURE : **DATE :**

Appendix 2

Acceptable Use Policy for Primary Pupils



To keep me safe whenever I use the internet or email, I promise…

- to keep my password private and not to use anyone else's login
- to keep my name, age, address and other personal information private
- not to click on any links or files that I do not understand or trust
- to tell an adult about any strange messages or upsetting internet pages
- to tell someone I trust if someone asks to meet me offline

- I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy
- I will use school computers for school work and not to upset or be rude to other people
- I will tell a teacher straight away if I see a website that is not my work or receive emails from people I don't know.
- I will look after school ICT equipment and tell a teacher straight away if something is broken or not working properly
- I will not try to download or install any software on school computers
- I will only use the username and password I have been given and I will keep them secret
- I will save only school work on the school network and will check with my teacher before printing
- I will log off or shut down a computer when I have finished using it
- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes nor change the settings
- I will not use chat and social networking sites unless I have permission from an adult
- I will not copy other people's work and pretend it is my own
- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website

If I break these rules…

- I understand that the school's behaviour guidelines will be followed

Appendix 3

Online Safety Incident Log Report

Reported By: *(name of staff member)*		**Reported To:**	
Date:			
Incident Description: (Describe what happened, where and who was involved)			
Action taken and outcome:			
Signature (Headteacher)		**Date:**	