



Foxton Primary School Online Safety Policy

School Name	Foxton Primary School
Date Approved	9 th July 2026
Review Date	July 2029

Agreed and Signed by Headteacher	
Name	Janet Muir
Agreed and Signed by Chair of Governors	
Name	Lisa Murphy

Support provided by



support@theictservice.org.uk | 0300 300 0000
www.theictservice.org.uk

"An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology"

(Keeping Children Safe in Education 2023)

It is essential that your Online Safety Policy shows your school's ability to:

- protect and educate pupils and staff in their use of technology
- have the appropriate mechanisms to intervene and support any incident where appropriate.

(Inspecting online safety in Schools, Ofsted 2014)

This policy considers guidance from:

- Meeting digital and technology standards in schools and colleges DfE March 2023
 - Teaching Online Safety in Schools guidance – DfE, January 2023
 - Education for a Connected World – UKCIS, June 2020
 - National Curriculum in England - Computing - DfE, Sept 2013
 - Relationships and Health Education – DfE, July 2020
-

Background to this policy

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practice embedded in our school and followed by the whole school community
- The infrastructure and how it is set up to keep pupils safe online, including filtering, monitoring, and preventing and responding to online safety incidents
- A progressive, relevant age-appropriate online safety curriculum for all pupils which meets the requirements of the National Curriculum for Computing and the statutory Relationships and Health Education

Online safety in schools is primarily a safeguarding concern and not a technology one. Therefore, this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

- **Safeguarding and Child Protection**
- **Personal Social and Health Education (PSHE)**
- **Safer Working Practices**
- **Data Protection / GDPR Policy**
- **Anti-Bullying Policy**
- **School Complaints Procedure**
- **Cambridgeshire Progression in Computing Capability Materials**
- **Whistle Blowing Policy**

This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

The development of our online safety policy involved:

- **The Headteacher**
- **The Designated Safeguarding Lead**
- **The Computing Subject Leader**
- **Cambridgeshire Local Authority Advisor (The ICT Service)**
- **The governor responsible for Safeguarding/computing**

This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff.

- All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As online safety is an important part of our school's approach to safeguarding, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

Rationale

At Foxton we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the misuse of technology can put users of technology at risk within and outside the school.

The risks they may face can broadly be categorised into the 4 C's; **Contact, Content, Conduct, and Commerce** (Keeping Children Safe in Education 2022) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing of Self-Generated Indecent Images
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming of music or video files
- Phishing or financial scams
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- **Staff laptops and iPads - staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.**
- **Staff / some staff have access to school systems beyond the school building (working via OneDrive).**
- **Peripherals such as Interactive Whiteboards**
- **Staff level internet access**

Pupils:

- **Curriculum laptops and iPads including filtered access to the Internet and pupil level access to areas of the school network**
- **Use of the interactive class whiteboard**
- **Information gained from the school website and suggested 3rd party websites used by the school. E.g. Times Table rockstars**

Where the school changes the use of existing technology or introduces new technologies which may pose risks to users' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

Devices at home:

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)
- Ensuring their hard drive is encrypted if possible – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Using the installed anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

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

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 Online Safety Lead.

The online safety curriculum

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the [National Curriculum for Computing \(England\)](#) and the statutory [Relationship and Health Education](#).

At Foxton we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

Our online safety curriculum is based around progressions of skills within the computing curriculum, based on the challenges of the 4Cs as referenced above, and the [Cambridgeshire PSHE Service Primary Personal Development Programme](#).

This is achieved using a combination of:

- Discrete and embedded activities within computing lessons, as one of the 3 computing strands identified in the computing curriculum, drawn from a selection of appropriate materials and is linked to demonstrating safe practice in our online learning platform
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as safe search practise, researching and communicating in appropriate online environments.
- Focus events to raise the profile of online safety for our pupils and school community e.g. NSPCC workshop 2025/26
- A flexible curriculum which is able to respond to new challenges as they arise.

Educating pupils about online safety:

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the [National Curriculum computing programmes of study](#). It is also taken from the [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

For more detail of below, please see computing curriculum overview

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

Pupils in **Key Stage 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

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
- How online imagery, media and accounts can provide misleading information that can effect mental health

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.

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 and in information evenings and events. This policy will also be shared with parents via our website.

Online safety will also be covered during parents' evenings.

The school will let parents 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
- An e-safety workshop will be delivered to the parents by the year 6 pupils in the summer term under the guidance of the e-safety lead

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.

Cyber-bullying

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

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. Teachers will discuss cyber-bullying with their tutor groups.

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 (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour 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.

Staff roles and continued professional development

In accordance with KCSiE guidance, staff at Foxton receive safeguarding and child protection training at induction. This training covers online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring. Safeguarding, child protection and online safety training is regularly updated during staff meetings and through updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.

Foxton will identify members of the senior leadership team (Janet Muir and Lynne Brooks), an E-safety lead (Aaron Marshall) and a governor (Lisa Murphy), to be responsible for ensuring the DfE filtering and monitoring standards are met. These identified individuals will receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.

Roles and responsibilities:

The governing board

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).

The governor who oversees online safety is Lisa Murphy.

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 ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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 being implemented consistently throughout the school. In addition, to log any incidents as reported by the monitoring systems if relevant.

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and Deputy DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school.

In addition, to log any incidents as reported by the monitoring systems if relevant.

The Online Safety Lead

The OSL is responsible for:

- Monitoring and updating security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis, alongside the ICT services who provide this service.
- To communicate with the ICT services to ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensure a full security check and monitoring the school's ICT systems on a termly basis or as required are performed by the ICT Service.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- In addition, to log any incidents as reported by the monitoring systems if relevant.

This list is not intended to be exhaustive.

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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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'

This list is not intended to be exhaustive.

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 ICT systems and internet (appendices 1 and 2)

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](#)

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, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

At Foxton, filtering services are provided by the ICT services and monitored by the above-named members of staff. Any instances of blocked materials are discussed with class teachers, e-safe lead and if needed the children and parents.

Mobile phones and use of mobile data in school

Keeping Children Safe in Education acknowledges that “many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G).” It highlights the need for schools to have a clear policy statement on, and carefully consider *“how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.”*.

Pupils may bring mobile devices into school, but are not permitted to use them during school time. This must be arranged in advance with the headteacher. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Monitoring and averting online safety incidents

The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following Safeguarding procedures where appropriate.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. Safeguards built into the school's infrastructure include:

- Secure, private EastNet internet connection with a direct link to the National Education Network. This is provided and maintained The ICT Service on behalf of the local authority.
- Managed firewalling running Unified threat management (UTM) that provides restrictions on download of software, apps and file types from known compromised sites.
- Enhanced web filtering provided to all EastNet sites as standard.
- Antivirus package provided as part of EastNet Connection.

Staff also monitor pupils' use of technology and, specifically, their activity online. This is achieved through a combination of:

- Appropriate levels of supervision when pupils are using online technologies
- Auto-generated alerts which flag up activity in specific safeguarding categories which may raise child protection concerns

Staff use of the schools' internet can also be monitored and investigated where needed.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network and OneDrive
- Visitors to the school can access part of the school systems using a generic visitor login and password.
- The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.
- School staff and pupils are not permitted to connect personal devices to the school's wireless network and a guest wireless key is issued to visitors on a case-by-case basis.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks to an acceptable level.

Pupils may bring mobile devices into school, but are not permitted to use them during school time. This must be arranged in advance with the headteacher. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Examining electronic devices

The headteacher, and any member of staff authorised specifically to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. This must always have the permission of the headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to Online Safety Lead and DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy

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

Responding to online safety incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.

If an online safety incident occurs, Foxton will follow its agreed procedures for responding, including internal sanctions and involvement of parents

In addition, the Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.

- With this in mind, the headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk and it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

However, at Foxton, incidents of this type are minimised as only Year 5/6 pupils have permission to bring a phone and it must be delivered to the office at the start of the day.

Our response:

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use of ICT. 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 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.

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the headteacher. At every review, the policy will be shared with the governing board. 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.

Appendix 1



Foxton EYFS and Key Stage 1 Acceptable Use Policy / Agreement

Author	e-Safety Co-ordinator Aaron Marshall
Version	
Version Date	July 2026
Status	Draft
Date Approved	07/07/26
Review Date	07/07/29

Agreed and Signed by Headteacher	[Insert Electronic Signature]
Name	Janet Muir
Agreed and Signed by Chair of Governors	[Insert Electronic Signature]
Name	Lisa Murphy

Support by



support@theictservice.org.uk | 0300 300 0000
www.theictservice.org.uk

My Online Safety Rules

- I only use the internet at school when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information safe.
- I will not share my passwords with anyone.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online.
- I always tell an adult/teacher/member of staff if something online makes me feel unhappy or worried.
- I will only use the camera on my device if asked to by an adult and will only take photos of things that do not upset people
- I know what might happen to me at school if I do not follow the rules:
 - Discussion with class teacher
 - Discussion with parents
 - Losing the right to use the devices at school
- I have read and talked about these rules with my parents/carers

Agreement

I am signing below to show that I have discussed this with my child and they understand that they must try to abide by these rules.

Pupils Name	
Parent/Carer Signature	
Date	

Appendix 2



Foxton Primary School Key Stage 2 Acceptable Use Policy / Agreement

Author	e-Safety Co-ordinator – Aaron Marshall
Version	
Version Date	July 2026
Status	Draft
Date Approved	09/07/26
Review Date	09/07/29

Agreed and Signed by Headteacher	[Insert Electronic Signature]
Name	Janet Muir
Agreed and Signed by Chair of Governors	[Insert Electronic Signature]
Name	Janet Muir

Supported by:



support@theictservice.org.uk | 0300 300 0000

My Online Safety Rules

- I will only use school IT equipment for activities agreed by school staff.
- I will only delete my own files unless my teacher gives me permission to delete someone else's. I will not look at other people's files.
- I will not use my personal email address or other personal accounts in school when doing school work.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- I will not deliberately look for, save or send anything that someone could find unpleasant or upsetting. If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts anything upsetting, unpleasant or nasty, about me or anything that makes me feel unsafe, I will not reply. I will tell my teacher, my parent/carer or another trusted adult immediately.
- I will not give out my own or other people's personal information such as name, phone number, home address, interests, schools or clubs. If I have to use a name online, I will use an anonymous nickname. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that could upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are, and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.

- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that no personal devices are to be used on school grounds.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that most of the above rules apply to the use of AI. In particular, I will not put any personal information, of myself or others, into AI and should always use AI functions with an adult present.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may:
 - Speak to me about my behaviour
 - Speak to my parents/carers about my use of technology
 - Remove me from online communities or groups
 - Not allow me to use laptops/computers or other mobile devices to access the internet, school computer network or particular programmes and apps.
 - Take any other action necessary to keep me and others safe.

Agreement

I am signing below to show that I understand and will try to abide by these rules.

Pupils Name	
Signed	
Date	

Appendix 3



Foxton Primary School Staff E-Safety Acceptable Use Policy / Agreement

Author	e-Safety Co-ordinator – Aaron Marshall
Version	
Version Date	July 2026
Status	Draft
Date Approved	09/07/26
Review Date	09/07/29

Agreed and Signed by Headteacher	[Insert Electronic Signature]
Name	Janet Muir
Agreed and Signed by Chair of Governors	[Insert Electronic Signature]
Name	Lisa Murphy

Supported by



support@theictservice.org.uk | 0300 300 0000
www.theictservice.org.uk

All staff should read and sign this document to demonstrate that they agree with the statements.

This policy covers the following aspects of e-safety in relation to all school staff:

- Use of school-based equipment
- Social Networking
- Managing digital content
- Email
- Mobile phones and devices
- Learning and teaching

School Policy

Modern technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school 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 technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students* 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 systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people. I understand that the rules set out in this agreement also apply to use of these technologies out of school, and to the transfer of personal data out of school.

Use of school-based equipment

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements.

- I will access the internet and other ICT systems using my personal username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the e-safety coordinator.
- All passwords I create will be in accordance with the school e-safety Policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems. (three words?)
- I will not share my passwords.
- I will seek consent from the e-safety coordinator/ headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-safety coordinator/ Headteacher/ DSL.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the network manager/e-safety coordinator (as appropriate)
- I understand my personal responsibilities in relation to the [Data Protection Act](#) and the privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g., by an open window or on the back seat of a car.
- Wherever possible I will use school provided cloud storage solutions to move files between devices. If I have to use a portable storage device (USB sticks, SSD cards, portable hard drives etc) I will ensure that it has been approved for use on the school network by the network manager/e-safety co-ordinator.
- I will ensure that any personal or sensitive information taken off site will be stored on a school-owned device with appropriate technical controls.
- Any information asset, which I create or have access to from other information systems, which could be deemed as personal or sensitive will be either stored on the school network or school provided cloud storage and access controlled in a suitable manner in accordance with the school data protection controls. (For example, spread sheets/other documents created from information located within the school information management system).
- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the network manager/e-safety co-ordinator.

- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the [Computer Misuse Act 1990](#) and breaches will be reported to the appropriate authorities.
- I understand that my files, communications and computer activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.
- I understand that the school digital technology 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.

Social Networking

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I will not use any social media tools to communicate with parents unless approved in writing by the Head Teacher.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- I know that staff must not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the e-safety coordinator.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school or for school use.
- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the e-safety Policy/ Home School Agreement (or any other relevant policy).
- Under no circumstances will I use any personally owned equipment for video, sound or images without prior consent from a member of the Senior Leadership Team.
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any [copyright licencing](#).
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally owned equipment.
- I will ensure that any images taken on school-owned devices will be transferred to the school network.

- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Email

- I will only communicate with parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will use my school email address for all email correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- Any personal device used to access school email or other communication systems will be encrypted and secured using a password in line with the school's password policy or biometric technology.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- I will comply with the privacy requirements of GDPR and the 2019 DPA when sending emails to groups of people by ensuring that all such emails are sent to Undisclosed Recipients.
- Emails sent to external organisations will be written carefully and if necessary, authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- I will ensure that I manage my email account and delete emails no longer required. Information I have a legitimate need to retain will not be kept in my email inbox but will be saved appropriately in the school's chosen storage system, ensuring access for other users if appropriate.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

Mobile phones and devices

- I will ensure that my mobile phone and any other personally owned device is switched off or switched to 'silent' mode during school hours.
- Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances. If I have to

keep Bluetooth turned on, I will ensure that the connection has a name appropriate to the setting.

- I will not contact any parents or pupils on my personally owned device.
- I will not use any personally owned mobile device to take images, video or sound recordings.
- All devices will be away from the teaching areas, in the designated staff spaces.

Learning and teaching

- In line with every child's legal entitlement, I will ensure I teach an age and stage appropriate e-safety curriculum.
- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources and the use of AI generated content at all times.

For AI please see the sperate policy.

Agreement

I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.

I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Name	
Role in School	
Signed	
Date	
Accepted by	
Date	

Appendix 4



Foxton Primary School AI Policy

School Name	Foxton Primary School
Date Approved	09/07/26
Review Date	09/07/29

Agreed and Signed by Headteacher	[Insert Electronic Signature]
Name	Janet Muir
Agreed and Signed by Chair of Governors	[Insert Electronic Signature]
Name	Lisa Murphy

Support provided by

support@theictservice.org.uk | 0300 300 0000

Contents

Aims	32
Legislation and guidance	32
Principles	32
Responsible Use of AI.....	33
Policy Review.....	33

Aims

Our school aims to ensure that Artificial Intelligence (AI) will be integrated responsibly into our activity. In this context AI refers to generative AI tools such as ChatGPT as well as other tools, both educational and administrative, that include AI features.

We will prioritise the safeguarding of our pupils and their online safety and will not knowingly use any AI technology that puts them at greater risk. Staff will not provide intellectual property, including pupils' work, to train Generative AI models without appropriate consents or exemptions in place.

Legislation and guidance

Foxton expects everyone who uses AI to comply with all relevant laws, regulations, policies and guidelines covering safeguarding, data protection, copyright and other relevant areas.

This policy takes account of statutory guidance included in Keeping Children Safe in Education and DfE guidance on Meeting Digital and Technology Standards in Schools and Colleges and is informed by the DfE guidance Generative artificial intelligence (AI) in education.

Principles

In implementing and using generative AI Foxton will follow these key principles:

Ethical Compliance: At Foxton we are aware that AI-generated content may possess biases or inaccuracies. We will always verify AI-produced results using trusted sources before considering them in academic work. We are committed to ensuring that whenever Generative AI is used bias of all forms will be addressed.

Transparency: We will ensure that pupils, staff, parents and other stakeholders are aware when and why Generative AI is used in school.

Privacy: We will comply with all current data protection legislation ensuring that parental consent is sought and obtained for the use of AI where necessary. We will safeguard all pupil, staff, and stakeholder data. Our Data Protection Policy can be found on our website.

Accountability: [Insert school name here] holds itself accountable for the implementation and development of AI systems. We will identify a member of the Leadership Team who will lead this work and will ensure compliance with this policy.

Access: We will only allow the use of AI with pupils when it has been demonstrated that its use will enhance the experience of students and could improve their outcomes.

Workload: At Foxton we look for ways to better manage the workload of our staff. We will only implement AI when it has been shown that to do so will reduce the demands on staff.

AI should enhance, not replace, human creativity. Examples include but are not limited to lesson planning, quiz creation, and flashcard generation.

Responsible Use of AI

- Staff must not share personal data with AI tools without approval.
- Staff can use AI tools to support their work as long as no personal data is shared with the tool. Staff must be open and transparent with their colleagues when they have used generative AI to produce curriculum materials. This will allow colleagues to check the reliability and veracity of the resources produced.
- Staff wanting to use AI must conduct a risk assessment in the form of a GDPR compliant DPIA to assess the threat to personal data. Approval to use an AI tool will only be granted when a DPIA has been completed and needs to be agreed by our DPO.
- Staff are expected to use their professional judgement to check any AI generated content for accuracy, bias and relevance before it can be used in the classroom. Staff must not use AI generated content where they have not carried out necessary and appropriate checks.
- Pupils will be taught about the opportunities and risks arising from the use of Artificial Intelligence in ways appropriate to their age and educational key stage.
- Pupils will be taught the importance of critical thinking, creativity and originality in their work. Pupils who use generative AI to produce work must acknowledge and reference the tools they have used and the work that it has produced.
- Pupils will be taught how to use generative AI ethically and to avoid it being misused.
- Pupils will be taught about the threats posed by AI and will be expected to apply the knowledge they have regarding copyright, intellectual property and plagiarism to ensure that their use of AI is ethical and legal and complies with the existing legal framework.
- Pupils will be taught how to keep themselves and others safe whilst using AI and will be expected not to use AI in an unsafe manner. Whenever a pupil uses AI in an unsafe way that causes harm to themselves or others, they will be dealt with in accordance with the school's behaviour policy.

Policy Review

At Foxton we understand that AI is a rapidly developing technology. What is seen as good practice today might be regarded as dangerous in the future. This policy will be kept under review by the leadership team and will be formally reviewed on an annual basis.

Appendix 5: Cambridgeshire & Peterborough Safeguarding Partnership Board Procedure

Where the school suspects that an incident may constitute a safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated in the diagram below.

If you think that a child or young person is at risk of serious harm contact Children Social Care <https://safeguardingcambspeterborough.org.uk/concerned/>

Out of hours emergencies 01733 234724.

Online Safeguarding Incident
“A Safeguarding incident where technology is involved”

Pass on to Designated Person/
Safeguarding Lead and record the incident

Is the child / young person or any other individual in immediate physical / sexual danger?

Report to Police
999

The child / young person is not in immediate danger

Report to Police
101

The incident involves an adult working with children / young people

[Follow Managing Allegations or Serious Concerns in Respect of Any Adult who Works or Volunteers with Children procedures](#)

A member of staff or volunteer is the victim

Consult your Manager or Senior Lead. If they are not available, consult your HR provider

Secure any evidence (equipment/images etc.) if safe and possible to do.
DO NOT view or copy if images or messages are of a sexual nature

Take advice from Safeguarding Lead in your own agency

[Follow Safeguarding Procedure](#)

Follow Internal Procedure

Throughout this process, please ensure that all those involved are supported appropriately