Online Safety, Filtering, Monitoring and Cyber Security Policy

Date effective	July 2026
Review Cycle	2 Yearly
Review Date	July 2028
Date of Approval by Governors	July 2026
Committee approved by	Foxford Local Governing Body
Author	Bruce Rogers

Date	Notes

1. Introduction

Foxford Community School understands that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open opportunities for pupils and play a significant role in their everyday lives.

Whilst the School recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

The School has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The School is committed to providing a safe learning and teaching environment for all pupils and staff and has implemented controls to reduce any harmful risks.

This policy will be updated as necessary to reflect best practice, amendments made to legislation, Keeping Children Safe in Education, DfE digital and technology standards, local/trust safeguarding expectations and emerging technology risks. It will be reviewed annually and may be reviewed sooner following a significant safeguarding, online safety, filtering/monitoring or cyber security incident.

"Users" – Any person including staff, students or external
"Network Manager" – Senior ICT Technical Lead person
"Staff" – Any person directly employed by the School
"Pupil" – Any pupil currently registered to the School

Safeguarding status and linked policies
Online safety is part of Foxford Community School's whole-school safeguarding arrangements. This policy should be read alongside the Child Protection and Safeguarding Policy, Behaviour for Learning Policy, Anti-Bullying Policy, Staff Code of Conduct, Data Protection Policy, Acceptable Use Policy, Remote Education Policy, Relationships and Sex Education Policy and any relevant Castle Phoenix Trust policies.
The Designated Safeguarding Lead has strategic oversight of online safety safeguarding risks, working with the senior leader responsible for online safety, the Network Manager, Trust IT and the Data Protection Lead/Officer where appropriate.

2. Considerations when using the internet

When accessing the internet, individuals are especially vulnerable to several risks which may be physically and emotionally harmful, including:

2.1. Access to illegal, harmful, or inappropriate images

2.2. Cyber bullying

2.3. Access to, or loss of, personal information

2.4. Access to unsuitable online videos or games

2.5. Inappropriate communication with others

2.6. Illegal downloading of files

2.7. Exposure to explicit or harmful content, e.g., involving radicalisation

2.8. Plagiarism and copyright infringement

2.9. Sharing the personal information of others without the individual's consent or knowledge

2.10. Exposure to misinformation, disinformation, conspiracy theories, online misogyny, discriminatory content, grooming, harmful challenges, fake or manipulated media, deepfakes, AI-generated harmful content and online financial exploitation or scams. Online safety risks will be considered through the 4Cs: Content, Contact, Conduct and Commerce.

3. Roles and responsibilities

3.1. It is the responsibility of all users to ensure that the internet, is used in an appropriate and legal manner. If any users are witnesses to or believe that ANY illegal or harmful activities have taken, or are taking place, they MUST inform an appropriate member of staff immediately.

3.2. The network manager is responsible for the implementation and day to day management of the safety systems and software used within the School and managing any issues that may arise. This includes ensuring that appropriate filtering is in place for all users and that this is up to date.

3.3. The network manager will provide technical support and advice to members of staff as required and will support any wider School CPD.

3.4. The Assistant Headteacher will ensure there is a system in place which monitors and supports the network manager, whose role is to work with the Designated Safeguarding Lead (DSL) to carry out the monitoring of e-safety in the School, keeping in mind data protection requirements.

3.5. The network manager will maintain a log of submitted e-safety reports, incidents, and technical issues. All incidents and issues will be reported to the Assistant Headteacher, Designated Safeguarding Lead (DSL) and the Trusts Data Protection Lead (DPL) as appropriate.

3.6. The school will ensure that all members of staff are aware of the procedure when reporting ESafety incidents.

3.7. The network manager and Assistant Headteacher will carry out regular reviews of internet usage data by all users and address any concerns as they arise. Proactive monitoring MUST take place and the appropriate staff member MUST be alerted directly and automatically of any incidents.

3.8. Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying Policy.

3.9. Teachers are responsible for ensuring that e-safety is embedded in the curriculum and safe internet access is always promoted.

3.10. All staff and pupils will ensure they understand and adhere to the school's Acceptable Use Policy, which they must sign and return to the School. The School MUST keep a log of acceptance and this must be updated as changes occur.

3.11. All pupils MUST be made aware of their responsibilities regarding the use of the school's ICT systems and equipment, including their expected behaviour.

3.12. The School MUST meet the minimum requirements of the GDPR ICT Audit or better. If you are unsure or believe that the School no longer meets this requirement you must inform the DPO immediately.

Governance, assurance and annual filtering/monitoring review
The Local Governing Body, through the safeguarding link governor, will receive at least annual assurance that filtering and monitoring systems are effective, proportionate and aligned with the school's safeguarding context.

The annual review will include the DSL, senior leader responsible for online safety, Network Manager and Trust IT/DPO where appropriate. Evidence should include the date of the review, systems in use, alert triage process, escalation routes to the DSL, incident trends, blocked/allowed site requests, over-blocking/under-blocking considerations and any actions required.

Filtering is preventative and monitoring is reactive. Both must be understood by safeguarding and technical staff so that pupils are protected from illegal, inappropriate and potentially harmful content without unreasonably restricting teaching and learning.

4. eSafety education

4.1. Educating pupils:

4.1.1. The School will regularly update pupils to make sure they are aware of the safe use of new technology both inside and outside of the School.

4.1.2. Pupils will be taught about the importance of online safety and will be encouraged to be critically aware of the content they access online, including extremist material, misinformation, disinformation, conspiracy theories, harmful or discriminatory content, fake/manipulated media, deepfakes, AI-generated content and the validity and reliability of website content.

4.1.3. Pupils will be taught to acknowledge information they access online, to avoid copyright infringement and/or plagiarism.

4.1.4. Clear guidance on the rules of internet use will be present in all classrooms where ICT is used.

4.1.5. Pupils are instructed to report any suspicious use of the internet and digital devices to a member of staff.

4.1.6. The school will promote online safety through curriculum provision, tutor time, assemblies and events such as Safer Internet Day and Anti-Bullying Week. Online safety education will be age-appropriate and will support pupils to understand content, contact, conduct and commerce risks.

4.2. Educating staff:

4.2.1. E-safety training opportunities MUST be available to all staff members, including whole School activities and CPD accredited training courses where appropriate.

4.2.2. All staff will undergo online safety training, including cyber security, filtering and monitoring awareness, data protection, safeguarding reporting routes and emerging technology risks such as generative AI and deepfakes, on an annual basis and as part of induction.

4.2.3. All staff will undergo ongoing phishing training by the School that will identify individual CPD needs of staff.

4.2.4. All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

4.2.5. All staff are reminded of the importance of acknowledging information they access online, to avoid copyright infringement and/or plagiarism.

4.2.6. Any new staff are required to undergo online safety and awareness training as part of their induction programme, ensuring they fully understand this policy.

4.2.7. The Network Manager will act as the first point of contact for staff requiring general safety advice. Safeguarding issues or concerns MUST be processed using the school's safeguarding processes.

5.Control Measures

5.1. Internet Access

5.1.1. Internet access will be authorised once parents and pupils have returned the signed consent form in line with The Trust's Acceptable Use Policy.

5.1.2. A record will be kept by the School of all pupils who have been granted internet access.

5.1.3. All users in Key Stage 3 and above will be provided with usernames and passwords and must keep these confidential to avoid any other pupils using their login details.

5.1.4. Management systems may be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.

5.1.5. Keeping Children Safe in Education compliant filtering and monitoring systems MUST be in place and in use to reduce potential risks to pupils through access to, or attempts to access, websites or content which may be illegal, inappropriate or harmful. This includes text, images, audio, video, AI-generated content and other digital content formats.

Filtering and monitoring operation

Filtering and monitoring systems will be configured, reviewed and tested so they are effective for the age and needs of pupils, the school's curriculum, the devices and networks in use, and the school's safeguarding context.

Alerts from monitoring systems will be triaged promptly by appropriate staff and escalated to the DSL where there is a safeguarding concern. The school will maintain records of significant alerts, decisions and actions in line with safeguarding and data protection expectations.

5.1.6. Any requests by staff for websites to be added or removed from the filtering list must be authorised by the Network manager and logged.

5.1.7. All School systems MUST be protected by up-to-date anti-virus software.

5.1.8. An agreed procedure will be in place for the provision of temporary users, e.g., volunteers.

5.1.8.1. These accounts MUST be assigned to a single user and logged to ensure that in the event of any abusive, illegal, or behavioural matter can be investigated and allow the investigating office to identify a single individual.

5.1.9. If authorised by the Headteacher, staff can use the internet for lawful and appropriate personal use during out-of-School hours, as well as break and lunch times. **Please Note:** All internet activity on School devices will leave a digital footprint. Any person choosing to use School devices for personal reasons is giving permission for the School to have this data until such time that the digital footprint is purged.

5.1.10. Personal use will only be monitored by the network manager, HR (Human Resources) or safeguarding staff for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so and would outweigh the need for privacy.

5.1.11. Inappropriate internet access by a member of staff may result in the staff member being restricted.

6.Social Networking

6.1. Please note: Additional detail is provided in the Staff AUP

6.2. Use of social media on behalf of the school will be conducted following the processes outlined in The Trust's Social Media Policy.

6.3. Access to social networking sites will be filtered as appropriate.

6.4. Should access be needed to social networking sites for any reason, this will always be monitored and controlled by staff and must be first authorised by the Headteacher.

6.5. Staff are not permitted to publish comments about the School/Trust which may affect its reputability.

Emerging technologies and artificial intelligence

The school recognises that emerging technologies, including generative AI, image/video manipulation tools, deepfakes, automated content generation and new social platforms, may create safeguarding, data protection, academic integrity and cyber security risks.

Staff and pupils must not upload personal, confidential, safeguarding or assessment information into unauthorised AI tools or external platforms. Use of AI tools for educational purposes must be lawful, transparent, age-appropriate, safe, and aligned with school/trust acceptable use, data protection and safeguarding expectations.

Concerns involving AI-generated harmful content, impersonation, manipulated media, online harassment or misuse of pupil/staff data must be reported through the school's safeguarding and/or data protection processes as appropriate.

7.Published content on the school website and images

7.1. The Assistant Headteacher and Network Manager will be responsible for the overall content of their school website and will ensure the content is appropriate and accurate.

7.2. Contact details on the school website will include the phone number, email and address of the school.

7.3. Images and full names of pupils, or any content that may easily identify a pupil, must follow the School/trust policies relating to the Data Protection Act 2018.

7.4. Pupils are not permitted to take or publish photos of others without permission from the individual and the School.

7.5. Staff can take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.

7.6. Any member of staff that is representing the school online, e.g., through blogging, must express neutral opinions and not disclose any confidential information regarding the School, or any information that may affect its reputability.

8. Mobile devices and hand-held computers

8.1. The Headteacher, Assistant Headteacher and Network Manager may authorise the use of mobile devices for a pupil and staff where it is seen to be for safety, precautionary or educational use.

8.2. If permitted, pupils and staff will access the school's Bring You Own Device (BYOD) Wi-Fi system using their personal mobile devices and hand-held computers providing the user and/or device meets the academies individual criteria. Internet access will be monitored for any inappropriate use by the network manager when using these on the school premises. The school does not have responsibility for any devices brought into school.

8.3. Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the network manager and/or DSL when using these on the school premises.

8.4. Using the school's devices or network to send inappropriate messages or images is prohibited.

8.5. Personal mobile devices will not be used to take images or videos of pupils or staff.

9. Cyber bullying

9.1. This section must be reviewed alongside the School's "Anti-Bullying Policy"

9.2. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

9.3. The Trust recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

9.4. The School will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

9.5. The School will commit to creating a learning and teaching environment which is free from harassment and bullying, for all staff and pupils.

9.6. The Headteacher will decide whether it is appropriate to notify the police or other appropriate parties regarding the action taken against a pupil or staff member.

10. Reporting misuse

10.1. The Trust will clearly define what is classed as inappropriate behaviour in the Acceptable Use Policy, ensuring all pupils and staff members are aware of what behaviour is expected of them.

10.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to ESafety are explained to pupils as part of the curriculum in order to promote responsible internet use.

How to report an online safety concern

Students should report online safety concerns to a trusted adult, tutor, Year Leader, Assistant Year Leader, DSL/deputy DSL or any member of staff. Parents/carers should contact the school through the published

safeguarding/contact route. Staff must record and escalate concerns through the school safeguarding system without delay.

The school will respond to online safety concerns in a non-victim-blaming way. Children will not be treated as responsible for harm they have experienced online. If there is immediate risk of harm, emergency safeguarding procedures must be followed.

Misuse by pupils:
10.3. Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Headteacher.

10.4. Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.

10.5. Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the Headteacher and will be issued once the pupil is on the school premises.

10.6. Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with the "Child Protection and Safeguarding Policy" and reported to the Designated Safeguarding Lead (DSL).

Misuse by staff:
10.7. Any misuse of the internet by a member of staff should be immediately reported to the Headteacher.

10.8. The Headteacher will deal with such incidents in accordance with the "Allegations of Abuse Against Staff Policy" and may decide to take disciplinary action against the member of staff.

10.9. The Headteacher will decide whether it is appropriate to notify the police of the action taken against a member of staff.

11. Physical Security – Location Access

11.1. All on-site devices which store data MUST be kept in a secure location with appropriate access control for example a server room or hub room. Physical access to the server room must be limited to only those individuals who have legitimate responsibilities to justify such access. If the space is left unattended for ANY period, it MUST be secured before leaving. If keys are used, then the keys MUST not be suited to a master key and MUST be clearly marked "Do Not Duplicate"

11.2. Key allocations must be logged including the date provided. Any losses must also be logged with the appropriate person and key allocations must be fully audited annually.

11.3. Procedures must be in place to ensure access is removed when no longer required. Procedures must also be in place to address lost or stolen keys or access cards. All access to these locations must be audited and must include Names, Time, Date and Reason for access. This log must be kept for a minimum of the last 365 days

11.4. The school must ensure compliant arrangements are in place for the removal or relocation of any ICT equipment from its normal location. If temporary storage is required for equipment that contains ANY school data, then the chosen physical location must also meet the security requirements set out above. Note: these requirements relate to data storage only; you must also consider other policies such as health and safety.

12. Data Processing Equipment locations.

12.1. When considering screen locations for data processors the school MUST consider the ability to be "over seen". If there is any possibility of the data processors screen been "over seen" this issue must be addressed before the device is used to process ANY school data.

12.2. Users MUST observe the following precautions when using a device to process data, or that has access to any school data:

12.2.1. Devices are positioned in such a way that information being processed cannot be viewed by person(s) not authorised to view the information. Specific consideration should be given to the siting of devices on which high risk information is processed or retrieved and high traffic areas such as reception and other public spaces.

12.2.2. Devices MUST NOT be left logged-on when unattended for ANY period of time.

12.2.3. Accounts MUST NOT be shared with ANY other user for any reason.

12.2.4. Passwords MUST not be shared with any user, including technical staff. Note: Users may be asked to log into a device for technical staff to carry out maintenance or the technical staff may be required to change your password to carry out required work.

12.2.5. Users MUST NOT leave hard copies or unencrypted of "Personal Identifiable" digital data unattended at any time, including on the school grounds unless stored in a secure location that meets the physical security statements set out above. NOTE: Unattended data or data access is considered as a Data Breach and MUST BE reported to your local Data Protection Lead (DPL) for investigation by the Data Protection Officer (DPO).

12.2.5.1. For the sake of clarity, the statements above must be adhered to when accessing School Data from any device or at any location such as home, public space, friends and family homes, etc. Access to data MUST be secured from other unauthorised users at all times.

13. Inventory

13.1. A requirement of the Trusts building Insurance provider and to meet the obligations of the Data Protection Act 2018 increases the need for securing ICT equipment and each school must maintain and keep up to date an audit of ICT equipment.

14. Data Backup

This is led by the trust lead for Digital Security

14.1. All data must be backed up to a secure and GDPR Compliant offsite location. Any data that is taken off site or stored offsite for the purpose of back-up must be encrypted to a minimum of 256bit. At no point should all data including all back-up media exist in a single location.

Note: "Offsite" is defined as a location that is not geographically located to or have the same environmental concerns as the main school site.

14.2. Data stored as back-up MUST comply with the data retention policy. When data reaches "end of life" all data INCLUDING that stored in ANY backup file in ANY location MUST also be purged.

14.3. A back-up regime MUST allow for any individual piece of data to be recovered in a timely manner. It is accepted that some degree of data loss may occur, but this must not exceed more than data produced over the last 24 hours.

14.4. The school MUST conduct back-up testing as set out below (or better):

14.4.1. Daily – Confirm that the last back-up has completed successfully. Rectify any issues as necessary.

14.4.2. Half term – Data integrity check. This can be done by recovering a predefined number of files successfully. This will not require an official test if it has been carried out successfully for a real requirement.

14.4.3. Termly – Disaster Recovery Total loss test

14.5. Users may back-up their data individually, but this back-up must meet the required data security principles in this document.

14.6. The Primary back-ups should be carried out automatically at set intervals and information contained within these back-ups should only be accessible by the ICT Technical Team for verification and restoration. Other back-up methods can be used to allow users direct self-recovery of files in addition to a "Primary Back-up" but all backups must meet the storage and security requirements set out in this document.

14.7. The production environment must not be impacted by the running of back-up jobs. All backups must be created, scheduled and run according to the performance and availability requirements of the environment.

15. Malware and Virus Detection and Removal

15.1. Malware (malicious software) and Viruses can infiltrate your systems and software and cause damage or allow your systems to be used for malicious or unlawful activities.

15.2. All school devices MUST Use Anti-virus / Anti-malware detection and removal software at all times. This software MUST be set to scan on access for all devices and updates as a minimum of monthly. Where possible the software must be configured in such a way to stop unauthorised users from disabling it.

15.3. Users MUST NOT disable any Anti-virus/Anti-Malware software installed on their machine for any reason. If the user has an issue that they believe requires this to happen then they MUST contact a member of the technical team for support.

Mobile Devices (including school and personal laptops and mobile phones)

15.4. These devices MUST be encrypted and must be password protected. Encryption level must be equal to or exceed 128bit and the password MUST meet the Password Policy as stated above for laptops. Mobile devices can be secured in several ways but as a minimum MUST have a 4 Digit Pin or better.

15.5. Please note: that device accounts are for an individual's use and must not be shared. If another user requires access to the device this MUST be done using an appropriate account for the users and ensure that the user cannot access any data that they are not officially authorised to access.

15.6. All works devices MUST be encrypted, and password protected. When using mobile phones users must be aware of their surroundings and the ability to be "overheard" when discussing personal identifiable information.

15.7. Any device that is used to access or store school data including contact information or emails MUST be password and / or 4 Digit PIN protected as a minimum.

15.8. If this device is shared with other people outside of Foxford staff, then the device MUST be set in such a way that the data is not accessible by the other users. As this data is classed as offsite this data MUST be encrypted.

15.9. Mobile Phones and Tablets MUST be kept up to date with Apps and Operating Systems. It is the school's responsibility to ensure this is carried out for all school owned devices.
Users MUST ensure that their device meets this requirement.

Acceptable Use Policy

Responsible Use

The school has computers and Internet access to help your learning. These rules are to keep everyone safe and help us be fair to others. The rules below apply to the use of any of the school computers, devices, and wireless. They also apply whenever a user is logged on to the Foxford School network offsite, for example Microsoft Office 365.

- **Logins and Passwords** - Every person has a different computer login and password. You should never allow anyone else to use your details. Change your password if you think someone else may have your details. You must never use someone else's login details to gain access to the school network.

- **Personal Information** - Users are not allowed to share theirs or another's personal information, such as, date of birth, address, phone number.

- **Use of the Internet** - The internet is not to be used to access anything which is illegal, or anything that someone else may find offensive. This includes indecent images, extremist, or discriminatory material, racial or religious hatred. If you are unsure, or if you come across anything which makes you feel uncomfortable, you should turn your computer monitor off and let a teacher know.

- **Social Networking** - Never upload pictures or videos of others without their permission. It is not advisable to upload pictures or videos of yourself as they can easily be manipulated and used against you. You should never make negative remarks about the school or anyone within the school. Always keep your personal information private. Consider using a nickname and only inviting people you know. Universities and future employers search social networking sites in order to carry out background checks on students. Do not create, share or request fake, manipulated or AI-generated images, audio, video or text intended to harm, embarrass, impersonate, bully or mislead another person.

- **Extremism and radicalisation** – Individuals, groups and organisations with extremist and radicalised views use the internet to exert influence on young people. Do not access any websites or social network pages that promote such views. The school has systems in place to block extremist material and monitor students who try to access it. Any student found accessing such material will be reported to the relevant authorities.

- **Security** - you should never try to bypass any of the security in place, this includes using proxy bypass sites. This security is in place to protect you and other people on our network.

- **Etiquette** - Be respectful online; do not be abusive. Consider what you are saying, and how somebody else might read it as some things you write may be read incorrectly.

- **Mobile Phones** should always be kept out of sight. The only exception is when a teacher requires you to use your phone as part of a lesson. **Never take inappropriate pictures** of yourself and send to your friends or upload onto social networking sites. Never forward inappropriate pictures that you have received from somebody else.

- **Use of ICT in lessons** – ICT facilities must be used only as directed by the class teacher. Any other use of ICT during lesson time will be considered off task and sanctioned accordingly.

- **Cyber-bullying** – You must not transmit, re-transmit, publish, or store material on or through the Foxford school network or through your own property, which is bullying, threatening, abusive, hateful, indecent, or defamatory. Report incidents of cyber-bullying to a responsible adult.

- **ICT equipment** - Treat all school equipment with care and respect. Report any problems to a member of staff.

- **Disciplinary Action** – failure to follow this guidance, or deliberate misuse of school ICT, may result in a disciplinary action including recovery of damages, Police intervention, exclusion (fixed term or permanent).

Agreement and Understanding: By signing this document, the school assumes you have read and understood all the above. That you understand that any of your electronic communications and files could be looked at if they are related to yours or another's well-being. That you also I understand anything you report would be confidential and would help protect other pupils and yourself. If a pupil or user breaches the above rules, their account may be inspected, and their access stopped. They may also render themselves liable for disciplinary action up to and including, recovery of damages, Police intervention, and exclusion (fixed term or permanent).

Signature: _____**Date:** _____

Name in Capitals: _____