FOSTER'S PRIMARY SCHOOL

ONLINE SAFETY POLICY

Adopted on: 01/09/2026

Review Date: 01/09/2027

1. e-Safety Ethos

1.1 Aims and policy scope

Foster's Primary School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.

Foster's Primary School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Foster's Primary School has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

Foster's Primary School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of Foster's Primary School online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Foster's Primary School is a safe and secure environment.
- Safeguard and protect all members of Foster's Primary School community online.
- Raise awareness with all members of Foster's Primary School community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (RSE).

1.2 Writing and reviewing the online safety policy

The Designated Safeguarding Lead (DSL) is Mr Joe Elliott (Deputy Headteacher), who also leads the annual filtering and monitoring effectiveness review.

The Online Safety Policy and its implementation will be reviewed at least annually, and sooner following significant safeguarding incidents, changes to technology or relevant guidance. The DSL coordinates the review, the Headteacher retains overall operational accountability, and the governing body provides strategic oversight.

1.3 Key responsibilities for the community

1.3.1 1.3.1 The key responsibilities of the governing body and Headteacher are:

The governing body provides strategic oversight of online safety, assures itself that appropriate filtering and monitoring arrangements and staff training are in place, and scrutinises the outcomes and actions from the annual review.

The Headteacher has overall operational accountability for online safety, ensures that roles, resources and escalation routes are clear, receives the monthly School Protect report, and ensures that identified actions are completed.

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material.
- To work with and support technical staff in monitoring the safety and security of Foster's systems and networks and to ensure that Foster's Primary School network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole Foster's curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for Foster's Primary School community to access regarding online safety concerns, including internal, local and national support.

- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

1.3.2 The key responsibilities of the Designated Safeguarding Lead are:

The DSL leads safeguarding decisions arising from online safety incidents, including risk assessment, recording, appropriate referrals and liaison with children's social care or police where necessary.

As Deputy Headteacher and designated senior leader for filtering and monitoring reviews, Mr Joe Elliott coordinates and documents the annual effectiveness review with the Headteacher, Digital Learning Lead and technical support, reporting findings through school governance arrangements.

Safeguarding concerns arising from School Protect reports, SENSO notifications or staff reports are referred promptly to the DSL or deputy DSL; urgent concerns must not wait for the monthly report.

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends regarding online safety.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with Foster's Primary School lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitor Foster's Primary Schools online safety incidents to identify gaps/trends and use this data to update Foster's Primary Schools education response to reflect need
- To report to the school management team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Working with Foster's Primary School leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.3.3 The key responsibilities for all members of staff are:

All staff receive online safety and filtering and monitoring information at induction, regular safeguarding updates and role-appropriate training. Staff must report online safety concerns immediately through safeguarding procedures and must not investigate suspected criminal imagery themselves.

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of Foster's systems and data.

- Having an awareness of a range of different online safety issues and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrating an emphasis on positive learning opportunities.

1.3.4 The key responsibilities for staff managing the technical environment are:

Technical support implements and maintains the school's filtering and monitoring configurations, Jamf device management, network security and approved technical controls. It identifies failures or gaps, provides relevant technical reports and escalates safeguarding concerns to the DSL without delay. Technical support does not make safeguarding decisions.

The Digital Learning Lead supports curriculum integration, reviews educational applications and age-appropriate access, supports staff training in safe digital learning, and contributes educational expertise to the annual filtering and monitoring review.

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Maintaining and testing filtering configurations and monitoring arrangements in conjunction with the Headteacher and DSL; reporting changes, failures and safeguarding concerns promptly.
- Ensuring that the use of Foster's Primary School's network is regularly monitored and reporting any deliberate or accidental misuse to the Designated Safeguarding Lead.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority, London Grid for Learning (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the Designated Safeguarding Lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

1.3.5 The key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading Foster's Primary School Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.6 The key responsibilities of parents and carers are:

- Reading Foster's Primary School Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

2. Online Communication and Safer Use of Technology

2.1 Managing Foster's Primary School website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be Foster's Primary School address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.

2.2 Publishing images and videos online

- Foster's Primary School will ensure that all images and videos shared online are used in accordance with the school image use policy.
- Foster's Primary School will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, child protection, use of personal devices and mobile phones etc.
- In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

- All members of staff are provided with a specific Foster's email address to use for any official communication.
- The use of personal email addresses by staff for any official Foster's business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email (egress).
- Access to Foster's email systems will always take place in accordance to data protection legislation and in line with other appropriate Foster's policies e.g. confidentiality.
- Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Staff are encouraged to develop an appropriate work life balance when responding to email.
- Excessive social email use can interfere with teaching and learning and will be restricted. Access in school to external personal email accounts and social media is not allowed through the school network. See also the Social Media policy.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.

2.4 Official videoconferencing and webcam use for educational purposes

- The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- All videoconferencing equipment (including webcams built into laptops etc) will be switched off when not in use and where appropriate, not set to auto answer.
- Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users

- Pupils will ask permission from a teacher before participating in a videoconference call or message.
- Videoconferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent will be obtained prior to children taking part in videoconferencing activities.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.

Content

- The reason for the videoconference must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

2.5 Appropriate and safe classroom use of the internet and any associated devices

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
- Foster's Primary School's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability:
    - In EYFS, school-managed iPads and approved educational applications are used regularly within continuous provision, adult-led activities and planned learning, with developmentally appropriate adult guidance and supervision. In Year 1, pupils regularly access approved platforms and resources through teacher-directed activities and wider curriculum planning, with supervision reflecting their age, ability and needs.
    - From Year 2 upwards, pupils have access to individual school-managed iPads on a 1:1 basis during the school day. Across KS2, pupils use age-appropriate online tools and approved resources in teacher-directed and appropriately supervised activities. Individual device allocation does not permit unrestricted internet access. Pupil iPads remain on school premises.

School-managed iPads are centrally managed using Jamf and connect to protected school Wi-Fi; access to the private Wi-Fi password is restricted to key authorised staff. Appropriate filtering, monitoring, application

restrictions and teacher supervision are used together, with controls checked for the devices and connections in use. Authorised staff may use school-managed iPads off-site for professional purposes subject to school security and acceptable-use requirements.

- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools (LG*fL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search*) as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- Staff will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members of the school community to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by Foster's Primary School.
- Foster's recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff and parents/carers but requires that such technologies need to be used safely and appropriately within schools.

4.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies including safeguarding policy, the staff handbook and social media policy.
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. Foster's Primary School accepts no responsibility or liability for the loss, theft or damage of such items. Nor will Foster's Primary School accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used within Foster's Primary School by pupils and adults must only use in areas where no children are present – the staffroom, offices or classrooms while children are not present.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy.
- All members of Foster's School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene Foster's Primary Schools policies.
- Foster's mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.

4.3 Pupils use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- Pupil's personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during lessons and while moving between lessons. Children in Year 6 may bring their mobile phones into school if they are walking to or from school without an adult. They must be stored in the safes in the classroom and must not be accessed during the day. They will be returned at the end of the day. Foster's Primary School does not take responsibility for phones or other devices brought to school.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time
- If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Leadership Team.
- If a pupil needs to contact his/her parents/carers they will, under the discretion of the senior leadership team, be allowed to use a Foster's 'landline' phone.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will then only be released to parents/carers.
- Where a pupil device is suspected of breaching school rules, staff will act in accordance with the current Department for Education Searching, screening and confiscation guidance, the Behaviour Policy and safeguarding procedures. Any search or examination must be lawful, proportionate and justified; pupil or parental consent alone does not authorise unrestricted examination or deletion of content.
- Where indecent images of children, nude or semi-nude images or other potentially criminal material are suspected, staff must not intentionally view, copy, print, forward, share, save or routinely delete the material. Staff must not conduct their own investigation. They must secure the device where lawful and necessary, report immediately to the DSL or deputy DSL, and record the concern without reproducing the image. The DSL assesses risk and decides on safeguarding escalation, including referrals to children's social care or police where appropriate. Decisions about parents/carers, preservation of evidence and any removal of content follow current guidance and relevant agency advice.
- Where material may constitute evidence of a criminal offence, staff must preserve potential evidence, avoid unnecessary examination or alteration and seek DSL-led advice on police involvement and safe handling. The school will follow current DfE Searching, screening and confiscation guidance and UKCIS guidance on sharing nudes and semi-nudes.

4.5 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. data protection, confidentiality, data security, Acceptable Use etc.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.

- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches Foster's Primary School policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following Foster's Primary Schools allegations management policy.

4.6 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with Foster's Primary Schools acceptable use policy.

- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.

- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5. Policy Decisions

5.1. Reducing online risks

- Foster's is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.
- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school uses School Protect for filtering and monitoring reporting and SENSO for additional keystroke notifications and screen monitoring. The Headteacher receives a monthly filtering and monitoring report; concerns are communicated to the DSL for safeguarding assessment. High-risk alerts and urgent concerns are escalated promptly rather than held for monthly reporting.

The DSL, Mr Joe Elliott, coordinates a documented annual review of filtering and monitoring effectiveness with the Headteacher, Digital Learning Lead and technical support. The review considers the appropriateness of filtering rules, monitoring alerts and response, pupil vulnerabilities, educational access, device coverage, technical testing, incidents, changes in provision and training needs. The governing body receives appropriate assurance and oversight of resulting actions.

Technical support maintains filtering and monitoring configurations, verifies coverage across relevant devices and connections, and promptly reports outages, attempted circumvention and gaps in protection. Staff continue to supervise pupils; filtering and monitoring are not substitutes for safeguarding practice.

All pupil iPads are managed through Jamf and connect to protected school Wi-Fi with credentials available only to authorised key staff. Approved applications, access controls and age-appropriate restrictions are applied and reviewed. Pupil iPads remain on site; authorised staff use of school-managed iPads at home is subject to secure configuration and school policies. The school will verify the applicability of its filtering and monitoring controls to each device type and network connection.

Staff are trained to recognise and report concerns arising from internet use and monitoring notifications. The DSL records safeguarding decisions and referrals; technical staff document relevant technical action. Significant incidents, system changes or failures trigger an earlier review where appropriate.

- The school will take reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a Foster's computer or device.
- The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.

5.2. Internet use throughout the wider Foster's community

- Guests/visitors who needs to access the school computer system or internet on site must follow this policy.

5.3 Authorising internet access

- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

- An online safety (e-Safety) curriculum is established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- All users network and Internet use are monitored.
- Online safety (e-Safety) will be included in the PSHE, SRE, Citizenship and Computing programmes of study, covering both safe school and home use.
- Acceptable Use expectations and Posters will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.

6.2 Engagement and education of children and young people considered to be vulnerable

Foster's Primary School is aware that some children may be considered to be more vulnerable online due to a range of factors. The school will ensure that differentiated and ability appropriate online safety (e-Safety)

education is given, with input from specialist staff as appropriate (e.g. SENCO, Looked after Child Coordinator).

6.3 Engagement and education of staff

- The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

6.4 Engagement and education of parents and carers

- Foster's recognise that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Information and guidance for parents on online safety will be made available to parents in a variety of ways.

7. Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

7.2 Preventing and addressing cyber-bullying

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

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

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

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

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

8. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

9. Monitoring arrangements

The DSL logs online safety safeguarding concerns, actions and referrals; reviews patterns in School Protect reports and SENSO notifications; and coordinates the documented annual filtering and monitoring effectiveness review. The Headteacher receives monthly reporting, urgent concerns are escalated without delay, and the governing body receives appropriate oversight of findings and remedial actions.

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

Net Aware: www.net-aware.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

UK Safer Internet Centre: www.saferinternet.org.uk

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Online Compass (Self review tool for other settings): http://www.onlinecompass.org.uk/

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

Completed via Google Form provided on the below letter:

BEXLEY COUNCIL

FOSTER'S PRIMARY SCHOOL
WESTBROOKE ROAD WELLING KENT. DA16 1PN
Telephone 020 8298 7336 Fax 020 8298 7312 E-mail: admin@fosters.bexley.sch.uk
Headteacher: Mr J Hemley Deputy Headteacher: Mr J Elliott
Assistant Headteacher: Mrs K Freeman (KS1)
Phase Leaders: Miss L Smith (FS), Miss N Winter (LKS2) & Mr N Woods (UKS2)
School Business Manager: Mrs E Burca

Wednesday 24th June 2026

Digital Learning Agreement – KS1

Dear Parents and Carers,

We are inviting you and your child to read, sign and return the attached Digital Learning Agreement for Key Stage 1. This agreement supports our shared commitment to ensuring that your child can make the most of digital learning opportunities safely and responsibly.

As a school, we are committed to providing the tools, training and support needed to help every pupil succeed in their digital learning. However, to make this a truly successful experience, we also need the support and commitment of both pupils and parents.

The agreement outlines the school's responsibilities, the expectations we have for pupils and how you can support your child at home. By signing it together, we are reinforcing the importance of responsibility, care and the positive use of technology. This agreement will cover your child for the remainder of their time at Foster's in Key Stage 1.

Please note that pupils will only be issued with a personal iPad once this agreement has been signed by both the child and their parent/carer. The agreement must be signed and returned by Monday 13th July 2026.

As part of our commitment to creating an active and engaging learning environment, pupils will regularly use their iPads to take photographs and record their learning. This means that children may occasionally appear in photographs taken by their peers during classroom activities.

These images will only be shared securely within our learning platform, Showbie, to support learning, provide feedback and celebrate progress. By signing this agreement, you are giving consent for your child to:

- Use their iPad for learning activities, including taking photographs.
- Potentially appear in photographs taken by other pupils during lessons.
- Have these images shared securely with teachers via Showbie for educational purposes.

The link to your child's agreement can be found here: https://forms.gle/9F9kCSBdR4uHXsLz6

Should you have any questions or concerns regarding the Digital Learning Agreement, please do not hesitate to contact us via the school office.

Kind regards,

Mr Gregory and Mrs Freeman

Digital Learning Leads

BEXLEY COUNCIL

FOSTER'S PRIMARY SCHOOL
WESTBROOKE ROAD WELLING KENT. DA16 1PN
Telephone **020 8298 7336** Fax **020 8298 7312** E-mail: **admin@fosters.bexley.sch.uk**
Headteacher: Mr J Hemley Deputy Headteacher: Mr J Elliott
Assistant Headteacher: Mrs K Freeman (KS1)
Phase Leaders: Miss L Smith (FS), Miss N Winter (LKS2) & Mr N Woods (UKS2)
School Business Manager: Mrs E Burca

Wednesday 24th June 2026

Digital Learning Agreement – KS2

Dear Parents and Carers,

We are inviting you and your child to read, sign and return the attached Digital Learning Agreement for Key Stage 2. This agreement supports our shared commitment to ensuring that your child can make the most of digital learning opportunities safely and responsibly.

As a school, we are committed to providing the tools, training and support needed to help every pupil succeed in their digital learning. However, to make this a truly successful experience, we also need the support and commitment of both pupils and parents.

The agreement outlines the school's responsibilities, the expectations we have for pupils and how you can support your child at home. By signing it together, we are reinforcing the importance of responsibility, care and the positive use of technology. This agreement will cover your child for the remainder of their time at Foster's in Key Stage 2.

Please note that pupils will only be issued with a personal iPad once this agreement has been signed by both the child and their parent/carer. The agreement must be signed and returned by Monday 13th July 2026.

As part of our commitment to creating an active and engaging learning environment, pupils will regularly use their iPads to take photographs and document their work. This means that children may occasionally appear in photographs taken by their peers during group or classroom activities.

These images will only be shared securely within our learning platform, Showbie, to support learning, provide feedback and celebrate progress. By signing this agreement, you are giving consent for your child to:

- Use their iPad for learning activities, including taking photographs.
- Potentially appear in photographs taken by other pupils during lessons.
- Have these images shared securely with teachers via Showbie for educational purposes.

The link to your child's agreement can be found here: https://forms.gle/Y9grQnji61pnUc2H9

Should you have any questions or concerns regarding the Digital Learning Agreement, please do not hesitate to contact us via the school office.

Kind regards,

Mr Gregory and Mrs Freeman

Digital Learning Leads

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not: ● Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature ● Use them in any way which could harm the school's reputation ● Access social networking sites or chat rooms ● Use any improper language when communicating online, including in emails or other messaging services ● Install any unauthorised software ● Share my password with others or log in to the school's network using someone else's details	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**