Fairford C of E Primary School

Online Safety and Acceptable Use Policy

Approved by the Resources Committee May 2025. Next review October 2026 by the Resources Committee

Contents

Vision and Values

Our school vision is: ***Isaiah 49:16 "I have written your name on the palms of my hands".***
Actively learning together in a safe, happy environment shaped by the certainty that each individual is known and loved by God.

At Fairford Primary School we have chosen those values that best reflect our thoughts as a school and community

Perseverance
Friendship
Respect
Forgiveness
Trust
Thankfulness

1. Policy Aims

This online safety policy has been adopted by School, involving staff, learners and parents/carers.
It takes account of the current DfE statutory guidance *Keeping Children Safe in Education* and the DfE's *Early Years Foundation Stage Statutory Framework.*

The purpose of Fairford Primary online safety policy is to:

- safeguard and protect all members of Fairford Primary School community online;
- identify approaches to educate and raise awareness of online safety throughout the community;
- enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology; and
- identify clear procedures to use when responding to online safety concerns.

Fairford Primary School identifies that the issues classified within online safety are considerable but can be broadly categorised into four areas of risk, Content, Contact, Conduct, Commerce.

Content:
being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
Some online content is not suitable for children and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites. It's important for children to consider the reliability of online material and be aware that it might not be true or written with a bias.

Children may need help as they begin to assess content in this way. There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.

Contact:

being subjected to harmful online interaction with other users; for example:
peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

It is important for children to realise that new friends made online may not be who they say they are and that once a friend is added to an online account, you may be sharing your personal information with them. Regularly reviewing friends' lists and removing unwanted contacts is a useful step. Privacy settings online may also allow you to customise the information that each friend is able to access. If anyone has concerns that a child is, or has been, the subject of inappropriate sexual contact or approach by another person, it is vital that they report it to the police via the Child Exploitation and Online Protection Centre (**www.ceop.police.uk**). If a child is the victim of cyberbullying, this can also be reported online and offline. Children must be taught the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable, or if one of their friends is being bullied online.

Conduct:

online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Children need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. It's easy to feel anonymous online and it's important that children are aware of who is able to view, and potentially share, the information that they may have posted. When using the internet, it's important to keep personal information safe and not share it with strangers. We will teach children the importance of reporting inappropriate conversations, messages, images and behaviours and how this can be done.

Commerce:

risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Young people's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications. We will encourage children to keep their personal information private, learn how to block both pop ups and spam emails, turn off in-app purchasing on devices where possible, and to use a family email address when filling in online forms

2. Policy Scope

- Fairford Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Fairford Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Fairford Primary School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, extended schools services, 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 learners, parents and carers (who are referred to as "the community".)
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.1 Links with other policies, legal documents, practices and guidance.

This policy links with several other policies, practices and action plans including:

- Department for Education statutory guidance *Keeping Children Safe in Education*
- Department for Education's *Early Years Foundation Stage Statutory Framework.*
- Gloucestershire Safeguarding Children Partnership procedures
- Anti-bullying Policy
- Code of Conduct
- Positive Relationship and Behaviour Policy
- Prevent Policy
- Safeguarding and Child protection Policy
- Relationship and Sex Education (RSE) Policy
- Data Protection/GDPR Policy
- Social Media Policy
- Allegations of Abuse against Staff Policy
- Whistleblowing and Confidential Reporting Procedure

3. Monitoring and Review

- Technology in this area evolves and changes rapidly; Fairford Primary School will review this policy annually

- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.
- The named DSL will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning e.g. outcomes from Parent and Pupil Surveys.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (Julie Fellows, Headteacher) has lead responsibility for online safety.
- Whilst activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL.
- Fairford School recognises that all members of the community have important roles and responsibilities to play with regards to online safety. The Online Safety Team is made up of the Computing and E-safety Lead, the School Business Manager and The Technology Team, (3rd party organisation/IT provider).

4.1 The leadership, management team and Governors will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety and acceptable use; including a staff code of conduct/behaviour policy.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks; as schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have appropriate time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that there are appropriate risk assessments.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant, up to date knowledge required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Monitor records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms using MyConcern.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures using MyConcern.

4.3 The Computing and E-safety Lead will:

- Keep up to date with current research, legislation and trends regarding online safety and communicate this within the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches e.g. online safety presentations to parents and class newsletters.
- Report online safety concerns, as appropriate, to the headteacher and governing body.
- Work with the leadership team to review and update online safety policies annually with stakeholder input.
- Meet three times a year with the governor with a lead responsibility for Computing and e-safety/ online safety.

4.4 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to this Online Safety and Acceptable User Policy
- Take responsibility for the security of school systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.

- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's Safeguarding and Child Protection Policy and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally following the Safeguarding and Child Protection Policy).
- Take personal responsibility for professional development in this area.

4.5 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL (or deputy DSLs) and leadership team.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

4.6 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities.
- Contribute to promoting online safety in the school e.g. assemblies and e-safety competitions.
- Respect the feelings and rights of others both on and offline.
- Develop a responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.7 It is the responsibility of parents and families to:

- Read the Home School Agreement and encourage their children to adhere to its provisions.
- Support the school's online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.

- Contribute to the development of the online safety policies.
- Use the system Microsoft TEAMS, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- The school will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home amongst learners by:

  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in Personal, Social, Health and Economic (PSHE) and Relationship and Sex Education (RSE) teaching.
  - Teaching age appropriate online safety linked to the National Curriculum Computing objectives and Fairford School computing programme of study, alongside other resources. Framework is taught termly. In addition, teachers of all year groups look to exploit opportunities to address online safety issues throughout the computing curriculum.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching learners to be critically aware of the materials they read and showing them how to validate information before accepting its accuracy.

- The school will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
  - Displaying acceptable use posters.
  - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Providing online safety education and training as part of the transition programme across the key stages e.g. visits by the Police to Year 6.
  - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

- Fairford Primary School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational

Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

- Fairford Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum Fairford Primary School will seek input from specialist staff as appropriate, including the SENCO.

5.3 Training and engagement with staff

We will:

- Provide and discuss this Online Safety and Acceptable User Policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for staff on a regular basis, with at least annual updates.
    - This will be achieved through a blend of existing safeguarding and child protection training and updates, safeguarding newsletters or within specific online safety sessions, as deemed appropriate by the DSL and headteacher.
    - This will cover the potential risks posed to learners, (Content, Contact, Conduct and Commerce), as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures including the school's Safeguarding and Child Protection Policy.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside the school, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and families

- Fairford Primary School recognises that parents and families have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats.

- This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
- Drawing their attention to the Online Safety and Acceptable User Policy and expectations in newsletters, letters and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our Home School Agreement.

6. Reducing Online Risks

- Fairford Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
  - Regularly review the methods used to identify, assess and minimise online risks.
  - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices. Any exposure to unsuitable content must be reported to the DSL, Business Manager and Computing and E-safety Lead.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community.
- Staff must exercise caution when using information technology and be aware of the risks to themselves and others. Particular consideration must be given to any references to the school or anyone connected with the school bearing in mind the wide audience of any communication and the staff Code of Conduct.
- At all times act in accordance with the current *Keeping Children Safe in Education.*

7. Safer Use of Technology

7.1 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and sign the Online Safety and Acceptable User Policy before being given access to our computer system, IT resources or internet.

7.2 Decision Making

- Fairford Primary School governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.

- The governors and leaders are aware of the need to prevent “over blocking”, as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3 Filtering and Monitoring and Review

For filtering and monitoring to be effective it should meet the needs of all our pupils and staff and reflect our use of technology and minimise any potential risk from online material.

- Governors, Headteacher and SLT have overall strategic responsibility for meeting the standards. They will ensure that they understand and evaluate the changing needs and potential risk and will review the filtering and monitoring provision at least annually.

- The Headteacher and Designated Safeguard Lead Mrs Julie Fellows, a member of the senior leadership (SLT) team will review and discuss with the Governor responsible at least annually that our filtering and monitoring systems are working effectively and record the result from the online safety review and that the school is meeting safeguarding obligations.

  Should a safeguarding risk be identified, a change in working practise or new technology be introduced an additional review will be carried out.

- Checks to our filtering and monitoring provision will be written and recorded and will form part of our filtering and monitoring review process. These checks will also check for changes to the system setup to ensure that these have not been deactivated.
  The log will include:
  When checks undertaken
  Who did the checks
  What was tested & checked
  Actions needed

- Staff will receive appropriate training to ensure they understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring and know how to report and record concerns.

Our Filtering System:

- We will ensure that our filtering system blocks harmful sites but does not unreasonably impact on learning.

- Will not restrict students from learning how to assess and manage risk themselves.
- The school will use a reputable internet security provider.

- **7.4 Our Monitoring System**
  - Our DSL & DDSLs receive alerts when an incident occurs allowing prompt action to be taken and record the outcome.
  - Our monitoring strategy will be informed by our filtering and monitoring review and strategies implemented if required to minimise safeguarding risks on internet connected devices.
  - The DSL will take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.
  - We will appropriately monitor internet use on devices when they are in school. This is achieved by:

    Physical monitoring (supervision),
    Monitoring internet and web access (reviewing log information)

  - The management of technical monitoring systems will be managed by our third-party IT provider, The Technology Team, who will report to the DSL any concerns.
  - All staff are informed how to deal with any incidents which could be of a malicious, technical, or safeguarding nature and who should lead on any actions required.

  - If learners discover unsuitable sites, they will be required to:
    - Minimise the screen and report the concern immediately to a member of staff.
    - Follow the SMART rules:

- **S = SAFE**
- Keep safe by being careful not to give out personal information – such as your name, email, phone number, home address, school name to people who you don't know or trust online.
- **M = MEETING**
- Meeting someone you have only just been in touch with online can be dangerous. Only do so with your parent's or carer's permission and even then only when they can be present.
- **A = ACCEPTING**
- Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain nasty messages or viruses.
- **R = RELIABLE**
- Someone online might be lying about who they are, and information you find on the internet might not be correct.
- **T = TELL**
- Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable while using the internet

- The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputies) and/or technical staff e.g. IT support –The Technology Team
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.

- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF (Internet Watch Foundation), Gloucestershire Police or CEOP.

- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.5 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with the General Data Protection Regulation and Data Protection legislation.
    - Full information can be found in our Data Protection/GDPR Policy.

7.6 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Individual logins and passwords protecting the School's Server when accessing it off site. Only sharing the URL with staff members.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Using secure encrypted email systems such as 'Egress' to communicate personal and private information in accordance with the Safeguarding and Child Protection Policy.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - The appropriate use of user logins and passwords to access our network.
    - All users are expected to log off or lock their screens/devices if systems are unattended.

7.7 Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- We require all adult users to:
    - Use strong passwords for access into our system.

- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

7.8 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our school address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.9 Publishing Images and Videos.

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) this Online Safety and Acceptable User policy, the Code of Conduct (for staff) and the Social Media Policy.
- We will ask permission from parents to publish images and videos - this will begin at the start of the academic year in Early Years. If parents wish for images and videos of their child to be published, they must sign a consent form which is allocated by the school's administrator.

7.10 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including the staff Code of Conduct
  - The forwarding of any chain messages/emails is not permitted.
  - Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Staff will immediately inform headteacher or deputy headteacher if they receive any offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted

7.11 Staff email

- The use of personal email addresses by staff for any official school business is not permitted.

- All members of staff and Governors are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

7.12 Learner email

- Learners will receive education regarding safe and appropriate email etiquette before access is permitted.

7.13 Live Stream Lessons for Remote Learning

- Microsoft TEAMS is used as the only software to support and deliver Live Stream Lessons for remote learning.

7.14 Management of Learning Platforms

- Fairford Primary School uses Microsoft TEAMS as its official learning platform. The School Portal is also used to communicate with parents/carers.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff and/or learners leave the school, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator.
  - Access to the LP for the user may be suspended.
  - The user will need to discuss the issues with a member of the Senior Leadership Team before reinstatement.
  - A learner's parents/carers may be informed.
  - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of staff; in this instance, there may be an agreed focus or a limited time slot e.g. meetings.

7.15 Management of Applications (apps) used to Record Children's Progress

- Fairford School use Tapestry to track learners' progress and share appropriate information with parents and carers in Foundation Stage.
- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR).
- To safeguard learner's data:
    - Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
    - Devices will be appropriately encrypted or set with a password if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

- The expectations regarding safe and responsible use of social media applies to all members of Fairford Primary School.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Fairford Primary School community are expected to engage in social media in a positive, safe and respectful manner. Fairford Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control learner and staff access to social media whilst using school provided devices and systems on site.
    - Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

- Concerns regarding the online conduct of any member of Fairford Primary School community on social media, should be reported to the DSL (or deputy) and will be managed in accordance with our Anti-bullying, Conduct and Safeguarding and Child Protection policies.

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our Code of Conduct.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of Fairford Primary School on their personal social networking accounts; this is to prevent information on these sites from being linked with the school, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.

- Members of staff will notify the Senior Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- Advice is given regarding 'friends' on social media sites.
    - Staff should not 'friend' anyone where their only link is through school e.g. parent or governor.
    - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and the headteacher.
    - If ongoing contact with learners is required once they have left the school, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the headteacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputies).

8.3 Learners' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including the Anti-Bullying Policy and the Positive Relationship and Behaviour Policy
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be taught and advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the school and externally.

8.4 Official Use of Social Media

- Fairford Primary School official social media channels are:
    - Facebook
    - Twitter
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the headteacher.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use school provided email addresses to register for and manage any official social media channels.
    - Official social media sites are suitably protected and, where possible, are linked to/from our website.
    - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including this Policy, the Anti-Bullying Policy, the Conduct Policy, the Data Protection Policy and the Safeguarding and Child Protection Policy.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- We will ensure that use of any official social media does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
    - Have read and will adhere to the Online Safety and Acceptable Users Policy.
    - Always be professional and aware they are an ambassador for the school.
    - Disclose their official role *and/or* position but make it clear that they do not necessarily speak on behalf of the school.
    - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace including libel, defamation, confidentiality, copyright, data protection and equalities laws.

- Ensure that they have appropriate consent before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the school, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, learners, parents and carers.
- Inform their line manager, the DSL (or deputies) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

9. Use of Mobile Phones, and Smart Technology

9.1 Introduction

Fairford Primary School is committed to providing a safe, respectful, and distraction-free learning environment. While we recognise the increasing role of mobile phones and smart watches in everyday life, their use in school must be carefully managed to protect the welfare and focus of all pupils and staff.

This policy applies to **all school activities**, including **pre-school clubs, after-school clubs, off-site trips, and residential visits**. All pupils, staff, parents, visitors, and volunteers are expected to follow it. **Failure to comply may result in the enforcement of the Whistleblowing Policy, Disciplinary Procedures, and other relevant school policies.**

- **reference is made to DfE publication "Mobile phones in Schools"** **https://assets.publishing.service.gov.uk/media/65cf5f2a4239310011b7b916/Mobile_phones_in_schools_guidance.pdf**

9.2 Pupil Use

Mobile Phones

- Pupils are not permitted to bring mobile phones to school unless written parental consent has been given and approved by the Headteacher.
- Mobile phones may have a part to play in securing pupils' safety on their journey to and from school. Where a phone is required for this reason, it must be handed in to the class teacher at the start of the school day and collected at the end.
- Pupils' mobile phones must be clearly marked with their name to ensure easy identification.
- Mobile phones must remain switched off during school hours, pre-school and after-school clubs, and on off-site trips, unless permission is explicitly given by staff.
- Unauthorised use of a mobile phone will result in confiscation, and the phone will only be returned to a parent or guardian. Repeated incidents may lead to further disciplinary action.

- Pupils will be taught the risks that are associated with the use of mobile phones, both in school and more broadly, to ensure they understand the decision being taken by their school to prohibit the use of mobile phones throughout the school day.

Smartwatches

- Pupils are **not permitted** to wear smartwatches that have communication, recording, or internet access functions.
- Basic watches (without smart features) are allowed.
- If a smartwatch is used inappropriately, it will be confiscated and returned to a parent or guardian.

9.3 Staff Use

- Mobile phones must be switched to silent and not used during teaching time, meetings, school duties, or when supervising pupils, including during pre-school and after-school clubs and off-site trips.
- Staff may use mobile phones only in designated areas (e.g., the staff room) and only during non-teaching times.
- Personal mobile phones must not be used to take photographs or record pupils. Staff must use school-provided devices for any recordings or images.
- Smartwatches may be worn, but notifications must be disabled during teaching and supervision hours. Any camera function must be disabled at all times whilst in school or on school business.
- All staff will consistently enforce the school's policy on the use of mobile phones.

9.4 Parents, Visitors and Volunteers

- The use of mobile phones is not permitted in classrooms, corridors, or any area where pupils are present, including during pre-school and after-school club sessions and off-site trips.
- Phones must be set to silent or switched off while on the school premises.
- If a call must be taken, it should be done in a private area away from pupils.
- Photography and video recording on personal devices are strictly prohibited, unless authorised by the Headteacher for specific events.
- Smartwatches may be worn, but notifications must be disabled during time in school. Any camera function must be disabled at all times whilst in school or on school business.
- Should it be seen that a recording device of any nature has been used by a person whilst in school without specific permission, any member of staff can request for the footage to be immediately deleted. This includes recordings made during school performances and events.

9.5 Pre-school, After School Clubs and Off-site Trips

- This policy applies at all times, including before and after school when pupils are attending pre-school clubs, after-school clubs, and wraparound care.
- Pupils must not use mobile phones or smartwatches during these sessions.
- Staff, volunteers, and external club providers must follow the same rules as during the school day.

- On off-site trips and residential visits, pupils are not permitted to bring mobile phones unless approved by the Headteacher.
- If mobile phones are allowed on residential trips, their use will be limited to designated times set by staff. Any misuse will result in confiscation.
- Any mobile phone use during these sessions must be in line with **safeguarding and child protection policies**.

9.6 Responsibility and Liability

- The school accepts no responsibility for the loss, theft, or damage of any mobile phone or smartwatch brought onto school premises or on off-site trips
- Parents must ensure their child's mobile phone is clearly marked with their name to prevent mix-up Parents are advised to ensure that any necessary devices are appropriately insured

9.7 Enforcement and Consequences

- Failure to comply with this policy may result in disciplinary action under the school's Whistleblowing Policy, Disciplinary Procedures, and other relevant policies.
- Pupils who repeatedly fail to follow this policy will have their mobile phone/smartwatch privileges removed and further action may be taken in consultation with parents.
- Visitors or volunteers who do not follow the policy may be asked to leave the premises.
- The school reserves the right to review and update this policy in line with government guidance and best practice.

9.8 Contacting pupils during the school day

- Parents needing to contact their child during school hours **must do so via the school office**.
- During off-site trips, parents will be provided with a **designated emergency contact number** rather than contacting pupils directly.
- Pupils are not permitted to use mobile phones or smartwatches for communication during school hours or off-site trips unless explicitly allowed.

By following this provisions contained in this paragraph we ensure a **safe, respectful, and effective learning environment** for all pupils.

10. Officially Provided Communication

- The Office staff, teachers, teaching assistants and the school Site Manager have access to a school Walkie Talkies which remain on site and for the sole use of ensuring child safety.

- School Walkie Talkies will always be used in accordance with the Online Safety and Acceptable Use Policy and other relevant policies.

11. Responding to Online Safety Incidents and Concerns

- All staff will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All staff must respect confidentiality and the need to follow the official procedures for reporting concerns.
- Learners, parents and staff will be informed of our Complaints Procedure and staff will be made aware of the procedures contained in the school's Whistleblowing and Confidential Reporting Procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice.
- Where there is suspicion that illegal activity has taken place, we will contact the Gloucestershire Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local schools are involved or the public may be at risk), the DSL or headteacher will speak with Gloucestershire Police and/or Children's Social Care first to ensure that potential investigations are not compromised.

11.1 Concerns about Learners' Welfare

- The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL (or deputies) will record these issues in line with our Safeguarding and Child Protection Policy.
- The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

11.2 Staff Misuse

- Any complaint about staff misuse will be referred to the headteacher, in accordance with the Code of Conduct or the Allegations of Abuse by Staff Policy depending on the nature of the alleged misuse.

- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff Code of Conduct or the Allegations of Abuse by Staff Policy as appropriate.

12. Procedures for Responding to Specific Online Incidents or Concerns

12.1 Online Sexual Violence and Sexual Harassment between Children

- Our school has accessed and understood part 5 of *Keeping Children Safe in Education.* All staff have signed a document to say that they have read part 5.
- Fairford Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media and online sexual exploitation.
- Fairford Primary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Fairford Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Fairford Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our Safeguarding and Child Protection and Anti-Bullying Policies.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our Positive Relationship and Behaviour Policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police. If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the

wider local community. If a criminal offence has been committed, the DSL (or deputy) will discuss this with Gloucestershire Police first to ensure that investigations are not compromised.

- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

12.2 Youth Produced Sexual Imagery ("Sexting")

- Fairford Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.
- Fairford Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on/off site or using school provided or personal equipment.
- We will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our Safeguarding and Child Protection and related policies.
    - Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.

- Make a referral to Children's Social Care and/or the Police, as appropriate.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our Positive Relationship and Behaviour Policy but taking care not to further traumatise victims where possible.
- Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the Senior Leadership Team will also review and update any management procedures, where necessary.

12.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Fairford Primary School will ensure that all members of the community are aware of online child sexual abuse including exploitation and grooming, the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Fairford Primary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our Safeguarding and Child Protection policies and the relevant Gloucestershire Safeguarding Child Partnership's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.

    - Review the handling of any incidents to ensure that best practice is implemented; the Senior Leadership Team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using school provided or personal equipment.
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Children's Social Care and/or Police.
- If learners at other settings are believed to have been targeted, the DSL (or deputy) will seek support from the Police and/or Children's' Social Care first to ensure that potential investigations are not compromised.

12.4 Indecent Images of Children (IIOC)

- Fairford Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.
- If made aware of IIOC, we will:
    - Act in accordance with our Safeguarding and Child Protection Policy and the relevant Gloucestershire Safeguarding Children Partnership's procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as Children's Social Care , Gloucestershire police and the Internet Watch Foundation (IWF)

- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy DSL) is informed so that the matter can be reported to the Police, the LADO and Children's Social Care, as appropriate.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the school provided devices, we will:
    - Ensure that the DSL (or deputy DSL) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Care (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
    - Ensure that the headteacher is informed in line with our managing allegations against staff policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our Allegations of Abuse against Staff policy.
    - Quarantine any devices until police advice has been sought.

12.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Fairford Primary School.
- Cyberbullying is referred to in our Anti-Bullying Policy.

12.6 Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at Fairford Primary School and will be responded to in line with existing policies, including the Anti-bullying Policy and the Positive Relationship and Behaviour Policy.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy DSL) will obtain advice through Children's Social Care and/or Gloucestershire Police.

12.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our Safeguarding and Child Protection Policy and our Prevent Policy
- If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the Safeguarding and Child Protection Policy, the Prevent Policy and the Allegations of Abuse against Staff Policy..

13. Online Child on Child Abuse.

- Fairford School recognise that Child-on-child abuse can take various forms and include serious bullying, relationship abuse, domestic violence, child sexual exploitation, harmful sexual behaviour, and/or gender based violence. This form of abuse occurs when there is any kind of physical, sexual, emotional or financial abuse or coercive control exercised between young people. It includes bullying, cyberbullying, sexual violence, harassment and sexting. (Gloucestershire Safeguarding Children Partnership)
- Through the teaching of online safety, Fairford School will
    - Teach children to know and understand their rights, what to do if they are unhappy with something and what it means to give true consent.
    - Ensure children know the risks, talk about child on child abuse in an age appropriate way.

- If made aware of an incident involving peer on peer abuse, we will act in accordance with our Safeguarding and Child Protection Policy and Anti-Bulling Policy.

14. Useful Links for Educational Settings

National Links and Resources for Educational Settings

- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
    - ChildLine: www.childline.org.uk

- Net Aware: www.net-aware.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
  - UK Safer Internet Centre: www.saferinternet.org.uk