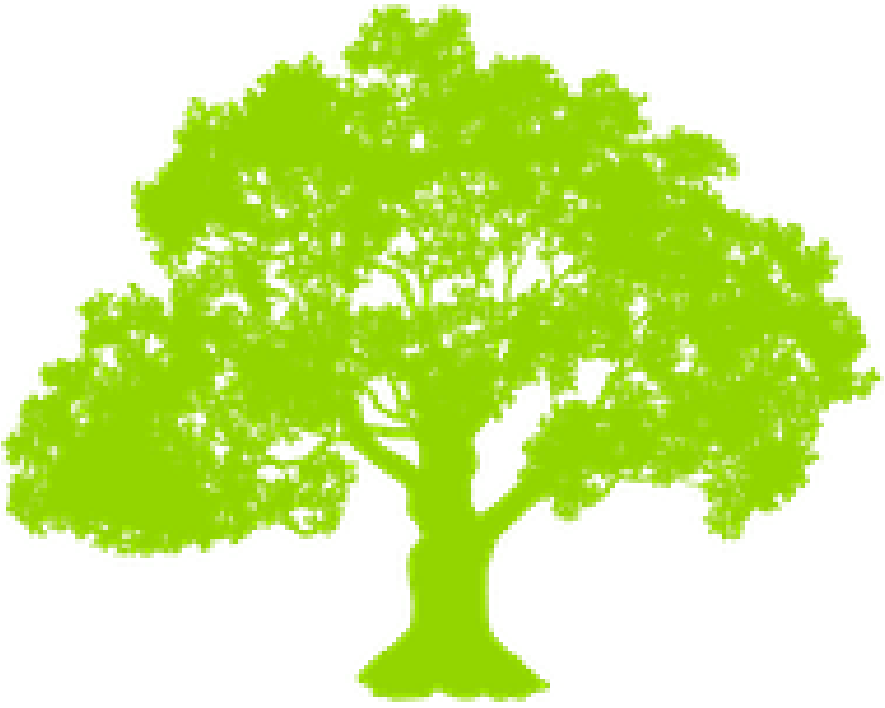
Fingringhoe

Church of England (VA) Primary School



Courage, Care, Compassion

Online Safety Policy

Date written: January 2025

Date of next review: January 2026

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure.

Contents

Fingringhoe C.E. Primary School Online Safety Policy

At Fingringhoe Primary School we understand the responsibility to educate our pupils in online safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy (for staff, governors, visitors and pupils), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Home-school agreements, Behaviour, Health and Safety, Child Protection, and PSHCE policies including Anti-bullying.

Our online safety policy has been agreed by the Senior Management Team and Staff. The online safety policy and its implementation is reviewed annually or when necessary, in line with national or local guidelines/changes, such as COVID 19.

1. Policy Aims

- This policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2024, Early Years and Foundation Stage 2017, 'Working Together to Safeguard Children' 2023 and the Essex County Council safeguarding procedures.

- The purpose of Fingringhoe C.E. Primary School's online safety policy is to:
    - Safeguard and protect all members of Fingringhoe C.E. 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, by modelling positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.

- Fingringhoe C.E. Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
    - Content: being exposed to illegal, inappropriate or harmful material
    - Contact: being subjected to harmful online interaction with other users
    - Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy Scope

- Fingringhoe C.E. 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.
- Fingringhoe C.E. 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.
- Fingringhoe C.E. 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, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy), as well as learners, parents and carers.
- 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 setting issued devices for use off-site, such as a work laptops, ipads or mobile phones.

2.2 Links with other policies and practices

- This policy links with several other policies, practices and action plans including:
- Code of conduct/staff behaviour policy
- Child protection policy

- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (SRE)
- Data security and GDPR
- Image use policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. Fingringhoe C.E. Primary School will review this policy at least 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 in conjunction with external technical support and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the *Head teacher* will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding *(Mary Josselyn)* 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.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (*Donna Parker and Hannah Coyle-Co Headteachers*) and Computing Subject Leader (*Laura Baker*) have lead responsibility for online safety.
- Fingringhoe C.E. Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governing Body	Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role Safeguarding Governor and this includes Online safety *(Mary Josselyn-Chair of Governors).*
Headteacher and Inclusion Leader	• The Headteachers have a duty of care for ensuring the safety (including online safety) of members of the school community. • The Headteachers are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. • The Headteachers are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Computing Coordinator	The Co-ordinator for Computing is responsible for: • Day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents. • Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place. • Providing training and advice for staff. • Liaising with the Local Authority. • Liaising with school technical staff. • Receiving alerts of online safety incidents on CPOMS. • Meeting regularly with Safeguarding Governor to discuss current issues. • Reporting to the Headteachers.
Network Manager/ Designated Safeguarding Person	The Network Manager (TCS)/Safeguarding Lead (Donna Parker and Hannah Coyle) is responsible for ensuring: • That the school's technical infrastructure is secure and is not open to misuse or malicious attack. • That the school meets required online safety technical requirements and any Essex County Council Online safety Policy or Guidance that may apply. • That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. • The Essex County Council filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. • That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of the network, internet, Virtual Learning Environment, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteachers.
Safeguarding Designated Person	The Headteachers and SEND coordinator should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from: • Sharing of personal data. • Access to illegal/inappropriate materials. • Inappropriate on-line contact with adults/strangers. • Potential or actual incidents of grooming. • Cyber-bullying.
Teachers	Teachers and Support Staff are responsible for ensuring that: • They have an up to date awareness of online safety matters and of the current school online safety policy and practices. Staff to be updated during staff meetings arranged with the Headteachers and relevant information to be given via school email addresses.

	• They have read and understood Staff Code of Conduct. • They report any suspected misuse or problem to the Headteachers for investigation/action/sanction. • All digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems. • Online safety awareness are embedded in all aspects of the curriculum and other activities, e.g. computing curriculum. • Pupils understand and follow the online safety policy. • Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and implement current policies with regard to these devices. • In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.1 The leadership and management team 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; including a staff code of conduct/behaviour policy, which covers acceptable use of technology.
- 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.
- 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 sufficient 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 appropriate risk assessments are undertaken regarding the safe use of technology.
- 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 settings 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 knowledge and up to date 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.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with 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. The school will provide opportunities within a range of curriculum areas to teach online safety. An online safety week is in place in line with national online safety week (usually February) whereby targeted age appropriate texts are read and discussed as part of reading sessions. Teachers are directed to tasks via https://www.saferinternetday.org/ which provides a focus and activities for teachers to do with their class. Other approved websites may be used in order to provide age appropriate awareness and activities to educate children.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the online safety curriculum. 'Kapow' scheme of work has been bought in (July 2020) which focuses on the three keys strands of computing including online safety.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the setting management team and Governing Body. Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (with the governor with a lead responsibility for safeguarding *and* online safety.

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

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting 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 settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally (CPOMS).
- Take personal responsibility for professional development in this area.

4.4 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 as directed by the DSL and leadership team to ensure that the settings 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.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.5 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 the development of online safety policies.
- Read and adhere to home school agreement which recognises the importance of safe internet use.
- Respect the feelings and rights of others both on and offline.
- Take 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.

4.6 It is the responsibility of parents and carers to:

- Read the home school agreement and encourage their children to adhere to the rules regarding online safety.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risks or concerns online.

- 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 setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in Personal, Social, Health and Economic (PSHE-Keeping Safe and Growing and Changing sections), Sex and Relationships Education (SRE) and computing programmes of study.
    - 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 shown how to validate information before accepting its accuracy.

- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
    - Displaying online safety posters in all rooms with internet access.
    - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

- Fingringhoe C.E. 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.
- Fingringhoe C.E. 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 Fingringhoe C.E. Primary School will seek input from specialist staff as appropriate, including the SENCO, Rachel Niven.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis as part of existing safeguarding training.
    - This will cover the potential risks posed to learners (Content, Contact and Conduct) 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.
- 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 of the setting, 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 carers

- Fingringhoe C.E. Primary School recognises that parents and carers 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 (e.g. the 2 Johns) and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
    - Requiring them to read our online safety policy and discuss the implications with their children.

6. Reducing Online Risks

- Fingringhoe C.E. 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.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material. Filtering of websites will be regularly monitored by our external technical support (TCS).
    - 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.
- 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. This is clearly outlined in our home school agreement and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- Fingringhoe C.E. Primary School uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices (e.g., iPads)
    - Internet which may include search engines and educational websites
    - Digital cameras, web cams and video recording devices
- All setting owned devices will be used in accordance with our staff code of conduct policy and with appropriate safety and security measures 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 setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. Children should always use a 'child safe' version of Google for searching.
- Supervision of learners will be appropriate to their age and ability.
    - Early Years Foundation Stage and Key Stage 1
        - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
    - Key Stage 2
        - Learners will use age-appropriate search engines and online tools.
        - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

7.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems in the form of our home school agreement.

- All staff and volunteers will read and sign a code of conduct policy, which outlines acceptable use of devices including the internet, before being given access to our computer system, IT resources or internet.

7.3.1 Decision Making

- Fingringhoe C.E. Primary School governors and leaders have ensured that our setting has age and ability-appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team and external technical support (TCS) will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- 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.

7.3.2 Filtering

- Education broadband connectivity is provided through Essex Education Services.
- We use a filtering system which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with Essex Education Services and our external technical support (TCS) to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - Report the concern immediately to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
    - 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, Essex Police or CEOP.

7.3.4 Monitoring

- 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.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

- Full information can be found in our information security policy, which can be found on our school website.

7.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly.
  - 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.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on our network.
  - 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.

7.5.1 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. Passwords will not be auto-saved and must be typed in separately each time.
- All learners (Reception-Year 6) are provided with their own username and password to access our systems; learners are responsible for keeping their password private. Student accounts have restricted access to specific files and have a filter applied to search engines (through United Net).
- We require all 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.

7.6 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 setting 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.

7.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the data security policy, including having parental permission for children's images to be published.
- Children whose parents have asked not to have their children's pictures published online, will be blurred or removed from photos.
- New parents will be asked to consent or decline to their child being viewed in photos for school purposes only.
- Parents who volunteer or attend performances will be advised not to post any photos on social media websites or take photos of other children other than their own.

7.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality and the code of conduct/behaviour policy.
    - 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.
    - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell the Head teacher if they receive offensive communication, and this will be recorded in our safeguarding files/records.

7.8.1 Staff email

- The use of personal email addresses by staff for any official setting 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 messages, especially if communication is taking place between staff, learners and parents.

7.11 Management of systems used to Record Children's Progress

At Fingringhoe C.E. Primary School, we use Target Tracker to record and monitor children's progress. The Head teachers are ultimately responsible for the security of any data 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) and Data Protection legislation.

- To safeguard learner's data:
    - Only school devices will be used to record and store learners' personal details and attainment.
    - Personal staff mobile phones or devices will not be used to access or upload content.
    - Devices will be appropriately encrypted with passwords 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.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Fingringhoe C.E. Primary School community.
- 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 Fingringhoe C.E. Primary School community are expected to engage in social media in a positive, safe and responsible manner.
    - All members of Fingringhoe C.E. 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 access to social media whilst using setting provided devices and systems on site.
- The online conduct of any member of Fingringhoe C.E. Primary School community on social media, should be reported to the DSL and will be managed in accordance with our behaviour policy, complaints procedure, and child protection policy.

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 policy.

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 setting.
    - 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 setting.
- Members of staff are encouraged not to identify themselves as employees of Fingringhoe C.E. Primary School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, 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 with 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 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

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputy).
    - If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use official setting provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted. Communication will be via official channels including DB Primary.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

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 and resources.
- We will ensure that learners and parents are aware that many popular social media sites state that they are not for children under the age of 13.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including our school 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 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 setting and externally.

9. Use of Personal Devices and Mobile Phones

- Fingringhoe C.E. Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting. Staff mobile phones will be on silent throughout the school day and personal use will only be permitted during staff breaks.
- Children are not permitted to bring mobile phones/smart watches to school unless agreed with the headteacher and must be left with the office on entering the school building and collected at the end of the day.

9.1 Expectations

- All use of personal devices (including but not limited to; tablets, smart watches and mobile phones) will take place in accordance with the law and other appropriate policies, such as behaviour and child protection policies.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.

    - All members of Fingringhoe C.E. Primary School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of Fingringhoe C.E. Primary School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of Fingringhoe C.E. Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and code of conduct policies.
- Staff will be advised to:
    - Keep mobile phones and personal devices are switched to silent or turned off, in a safe and secure place during lesson time.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless written/verbal permission has been given by the Headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
    - Keep personal phones in a secure place when off site and use only for school purposes during this time, e.g. PE on the field or outdoor classroom visits.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy).
- Staff will not use personal devices:
    - To take photos or videos of learners and will only use work-provided equipment for this purpose.
    - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct and complaints procedure policy.

- 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, the police will be contacted.

9.3 Learners Use of Personal Devices and Mobile Phones

- Fingringhoe C.E. Primary School expects learners' personal devices and mobile phones to be kept at the school office and switched off for the duration of the school day.
- If a learner needs to contact his/her parents or carers they will be allowed to use the telephone in the school office.
  - Parents are advised to contact their child via the school office phone or email address.
- Mobile phones and personal devices must not be taken into examinations.
  - Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place. These will only be released when collected after contact with the parents at the end of the school day.

9.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in school in accordance with our privacy policy and other associated policies, such as: behaviour and child protection.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) of any breaches our policy.

10. Responding to Online Safety Incidents and Concerns

- All members of the community 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 members of the community 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 whistleblowing 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 deputy) will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or Essex 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 settings are involved or the public may be at risk), the DSL or deputy will speak with Essex Police and the Education Safeguarding Team first to ensure that potential investigations are not compromised.

10.1 Concerns about Learners Welfare

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL (or deputy) will record these issues in line with our safeguarding policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Essex Safeguarding Children Board thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, in accordance with the code of conduct policy.
- 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.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2024 (most recent training given to all staff during INSET day September 2024).
- Fingringhoe C.E. 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.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our safeguarding policy.

- Fingringhoe C.E. Primary School recognises that internet use 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.
- Fingringhoe C.E. Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Fingringhoe C.E. 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 SRE curriculum (SCARF).
- 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 behaviour policies.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - 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 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 Work Service and/or Essex 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 Essex 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.

11.2 Youth Produced Sexual Imagery ("Sexting")

- Fingringhoe C.E. 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': "Responding to youth produced sexual imagery".

- Fingringhoe C.E. 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 respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting 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 policy and the relevant Essex County Council Safeguarding procedures.
    - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - 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 Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
        - 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 leadership team will also review and update any management procedures, where necessary.

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

- Fingringhoe C.E. 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.
- Fingringhoe C.E. 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.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our safeguarding policy and the relevant Essex Safeguarding procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Essex police via 101, or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of learner(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; 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 setting provided or personal equipment.
    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Team and/or Essex Police.

- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy).
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Essex Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- Fingringhoe C.E. 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 in conjunction with our technical support provider (TCS/United Net).
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Essex Police and/or the Education Safeguarding Team.

- If made aware of IIOC, we will:
    - Act in accordance with our safeguarding policy and the relevant Essex Safeguarding procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Essex police or the LADO.

- 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) 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 as well as to our technical support provider (TCS).
    - 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 setting provided devices, we will:
    - Ensure that the DSL (or deputy) 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 Work Service (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 setting provided devices, we will:
    - Ensure that the Headteacher is informed immediately in line with our managing allegations against staff policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
    - Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Fingringhoe C.E. Primary School.
- Full details of how we will respond to cyberbullying are set out in our behaviour policy.

11.6 Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at Fingringhoe C.E. Primary School and will be responded to in line with existing policies, including our behaviour policy and vexatious complaints 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) will obtain advice through the Education Safeguarding Team and/or Essex Police.

11.7 Online Radicalisation and Extremism

- All staff members have received PREVENT training and know how to recognise radicalisation.
- 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) will be informed immediately, and action will be taken in line with our child protection 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 safeguarding and code of conduct policies.