Fordham Church of England Primary School

Acceptable Use and Online Safety Policy

Statement Summary		
A synopsis of our school's approach to using IT and keeping children and staff safe online.		
	Date of writing	Summer 2026
	Date of review	Summer 2028
	Committee	Full Governors

Our School Christian Vision:

At Fordham, we are committed to achieving educational excellence by making learning stimulating, practical and above all, enjoyable. We believe in developing all God's children, allowing them to grow and 'flourish'. We aim to do this as a whole community where 'faith and friendship' are at the heart of our success.

KEY PERSONNEL:

Online Safety Lead: Louise Pack

Online Safety Governor: Rob Seal

Version Control

Date	Version	Amendments/comments	Reviewer(s)
March 2026	1.1	Updated Appendix Added Appendix 5 and 6	DR

Introduction:

At Fordham CE Primary, we recognise that information and communication technology plays an important part in learning and brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively and safely.

All stakeholders in school must use technology appropriately, safely and legally. We have a major responsibility to teach children the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies. This policy has links with, and works alongside the school's computing, child protection and anti-bullying policies.

All stakeholders should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that pupils, staff and volunteers will be responsible users and stay safe while using the internet and other technologies for educational, personal and recreational use.
- that school and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that pupils and staff are protected from potential risk in their use of technology in their everyday work.

A) <u>Responsibility for Appropriate use of ICT</u>

1. The Governing Body

- The school governing body have responsibility for ensuring that the school has an Acceptable Use 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. This policy is reviewed every three years.

- A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

  - Regular meetings with Online Safety Leader
  - Regular monitoring of the online safety incident logs

- Reporting to Governor meetings

2. Headteacher

- Headteacher oversees the Acceptable Use and Online Safety Policy ensuring that it is abided by.
- Headteacher ensures that procedures are followed and has an overview of Personnel files.
- Headteacher has a duty of care and is ultimately responsible for Online Safety for all members of the school community, including day to day responsibility for online safety.
- Headteacher will also be the Designated Safeguarding Lead (DSL) and will be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues that may arise.
- Headteacher should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Headteacher is responsible for ensuring that the Online Safety Lead receive suitable, up-to-date training to enable them to carry out their role.

3. Online Safety Lead

- To promote awareness and commitment to Online Safety throughout the school.
- To be the first point of contact on all Online Safety matters
- To take day to day responsibility for Online safety within school and have a leading role in establishing and reviewing the school's Acceptable use of ICT policy and procedures.
- To create, maintain and review Online Safety policies and procedures.
- To monitor online safety incidents to inform future online safety developments.
- To ensure that all staff are aware of the procedures that need to be followed in event of an online safety incident.
- The Online Safety Lead and IT Technician will ensure that all computers have up to date virus protection, monitoring software and an internet connection which is filtered through the regional broadband consortium (ENBN).
- The Online Safety Lead and IT Technician will meet on a regular basis to discuss monitoring and follow up any arising issues.

4. All staff

- All staff have a responsibility to use ICT appropriately and legally, and report any illegal or inappropriate use of ICT to the Principal or the Head of School/Online Safety Lead, as soon as possible.

- All staff must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

- Teachers and teaching assistants should address issues of online safety when using the internet with children.

- To educate the young people in our care in the safe use of digital technology.

5. **Volunteers and Visitors**

- Visitors and volunteers should ensure that all technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and children protection guidance, and the law.

- If they have any queries or questions regarding safe and professional practise online either in school or off site, they will raise them with the Designated Safeguarding Lead or Online Safety Lead.

- All volunteers and visitors to abide by the Acceptable Use Policy.

6. IT Technician

- To report any online safety related issues that come to your attention to the Online safety co-ordinator/Headteacher.

- To ensure that access to the school network is only through an authorised, restricted mechanism including guest access to networks.

- To restrict all administrator level accounts appropriately.

- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.

- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

- To ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack

- To ensure that the school meets required online safety technical requirements and Local Authority guidance that may apply.

7. Parents and Carers

- Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, national or local online safety campaigns. Part of our

communication to Parents/Carers will include reinforcing the legal age requirements for games/social media platforms and Generative AI.

- Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- handheld devices including mobile phones.

8. Pupils

- Pupils are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement for KS1 or KS2 (Appendix two and three).
- If they are bringing a mobile phone to school then their parents must complete a Mobile Phone Agreement (Appendix 5)

B) Education and Training

1. Teaching and Learning

All staff are required to uphold the highest standards of professional practice in teaching and learning. To ensure this, staff must:

- **Teach an age-appropriate and developmentally appropriate curriculum**, ensuring that learning is matched to pupils' needs, abilities and stages of development.
- **Promote and model the principles of the School's Online Safety Policy**, demonstrating safe, responsible and respectful behaviour when using digital technologies, and supporting pupils to do the same.
- **Understand and adhere to individual safeguarding responsibilities**, including the safe use of technology and the prevention, identification and reporting of any misuse or concerns.
- **Respect and acknowledge copyright, intellectual property and the appropriate use of AI**, ensuring that all digital content, resources and AI-generated materials are used ethically, legally and transparently.

2. Education – pupils

Whilst regulation and technical solutions are very important, their use must by balanced by educating pupils as well as parents and staff to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. It is a focus in all areas of the curriculum with online safety messages being reinforced and a planned online safety curriculum being followed as part of the computing and PSHE curriculum. Our online safety curriculum is based on the Kapow Scheme of Learning and Project Evolve with reference to UKCIS's Education for a Connected World. Online safety messages are also delivered in assemblies and special focus events e.g. Safer Internet Day.

Seesaw is a secure app that is used in school to supplement learning and share work, and essentially used as part of assistive technology. Permission to create accounts will be requested in a signed agreement by parents/carers. The teacher approves all posts before they are published and the children may demonstrate their digital citizenship skills by evaluating and communicating positively online. Only a child's initials are used throughout the app including when children, parents and staff comment.

Tapestry is a secure app used in EYFS at school and at home to show children's learning against the EYFS learning goals. Parents have signed a written agreement. All photographs of a child's learning are taken and posted by the class teacher. In accordance with school policy, a child's photo and their name do not appear together in a post. Parents can view their child's profile and add comments to their work.

TT Rockstars is a website used by the children to improve their times table knowledge. The children are given a secure password to access their accounts within school and at home. The class accounts are managed by the class teacher with password.

All other apps, website and software will not store the children's information and access will be as a guest. Parents and carers informed when new technologies are to be used.

Staff and pupils are not allowed to download or install software that could compromise the school network without prior authorisation.

Staff model safe and responsible behaviour in creation and publishing of online content p.6

3. Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

Curriculum activities
Letters, newsletters, web site,
Parents / Carers evenings / sessions
High profile events / campaigns e.g. Safer Internet Day, Safeguarding week
Reference to the relevant web sites / publications e.g. ***www.saferinternet.org.uk/*** ***http://www.childnet.com/parents-and-carers*** *https://www.ceop.police.uk/Safety-Centre/*

4. Education – Staff / Volunteers / Governors

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

Staff and Governors at Fordham CE Primary School receive up-to-date information and training on Online Safety issues in the form of strategy meetings and updates from the Online Safety Lead as well as training from external providers where appropriate.

All new staff, as part of their induction programme, are asked to ensure they fully understand this policy and have signed the Acceptable Use Agreements.

The Online Safety Lead will provide advice / guidance / training to individuals as required.

C) Access to ICT

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible. The ICT equipment is stored securely with only appropriate staff permitted access. Servers, workstations and other hardware and software will be kept updated as appropriate. Virus protection is installed on all appropriate hardware and will be kept active and up to date.

Files, communications and computer activity is monitored and checked with reports being sent to SLT to further investigate if required. School technology is intended for school use only.

All staff users will sign The Acceptable Use and Online Safety Policy provided by the school. Users must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.

Members of staff will access the curriculum network using an individual ID and complex password, which they will keep secure. They will ensure that they log out after each session and not allow pupils, or other adults, to access the internet through their ID and password. They will abide by the school AUP at all times and report any suspicion of breach of personal data.

At Key Stage 1, pupils will access the internet using a class ID and password, which the class teacher supervises. All internet access will be undertaken with a member of staff within the same room.

At Key Stage 2, pupils will access the internet using a class ID and password, in line with the pupil Acceptable Use Policy. They will ensure they log out after each session – this is overseen by the class teacher.

All users must not change another user's file without their permission.

D) Use of the Internet

The school encourages users to make effective use of the Internet. Such use should always be lawful and appropriate. Internet usage means any connection to the Internet via Web browsing, learning platform (including Seesaw and Tapestry), external email or news groups. The school has an obligation to fulfil its Prevent Duty and to ensure that no extremist or terrorist material can be accessed.

The school expects all users to use the Internet responsibly and strictly according to the following conditions:

Users shall not visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- Promoting extremism or terrorism
- promoting illegal acts

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in the UK
- extremist or terrorist material
- mistreatment of animals or animal abuse

Sites must not be accessed which contain inappropriate material defined below:

- Personal ads or dating
- Criminal skills or resources
- Internet based peer to peer networks e.g. Pirate Bay
- Downloads of ring-tones, screensavers and games
- Downloads of freeware, shareware or evaluation packages (excepting by authorised persons as designated by the school and in compliance with copyright law)
- Illegal drugs
- Hacking, virus writing or password cracking
- Gambling
- Depiction or avocation of violence or the use of weapons
- Breach of copyrights
- Instant messaging or online chat rooms not directly related to education or educational use.

Prohibited material will include any material which may be construed as offensive on the grounds of gender, race, ethnic origin, disability, sexuality, religion, age, HIV status, size, stature, trade union membership/office or any combination thereof or any group identified under the Equality Act 2012.

If inappropriate material is accessed accidentally, users should immediately report this to the Headteacher/ Online Safety Lead so appropriate action can be taken.

Access to internet web sites that are unrelated to school business should be restricted to out of school hours and designated breaks and should not leave a web history that through which children may access

inappropriate content. Where staff are unsure on whether given content is appropriate, they should contact the Online Safety Lead for clarity.

The use of YouTube as a teaching tool is allowed providing staff have vetted the video prior to the lesson to assess that the content is appropriate. Staff should use the freeze screen function when loading the video in case of any adverts appearing that could contravene this policy.

Collective worship may occasionally be delivered virtually using secure, pre-recorded videos ensuring that content cannot be accessed publicly. On rare occasions when Zoom or Microsoft Teams is used as a video-conferencing platform, sessions are fully supervised and protected with secure passwords.

Parent consultation meetings are facilitated through a dedicated, secure online platform organised by the school office, with staff conducting these meetings from the school premises rather than their homes.

When creating digital content—such as materials for collective worship or learning videos—staff must follow school expectations regarding safe, appropriate and professional use of technology.

MyConcern safeguarding platform is accessed only through secure log-in procedures, including multi-factor authentication, to ensure the highest level of data security and confidentiality.

E) Conducting Financial Activities on the Internet

While this policy does not ban the use of the internet for conducting personal financial transactions, e.g. e-banking, we warn against it on school machines. Residual information from such activities can be left on the computer hard drive and could subsequently be accessed by others. Similarly, personal or financial information may be inadvertently recorded by the school's monitoring software. The school or the local authority do not accept any liability for any resulting loss or damage.

F) Intellectual Property, Plagiarism and Copy Right

All staff and pupils must uphold the principles of intellectual property, ensuring that all online content is used legally, ethically and respectfully.

Any information, text, or digital material copied or downloaded from the internet and re-presented in any form must clearly acknowledge the original source. Only copyright-free, appropriately licensed or school-owned images and media may be used in teaching materials, digital content or online communications.

Plagiarism is not permitted under any circumstances, and all work published or shared within the school community must represent original effort or contain proper attribution. Staff should model these expectations to pupils at all times, including when preparing resources, producing learning videos or creating content for collective worship.

G) Email use

E-mail should never be sent, forwarded or replied to where the content is;

- Abusive
- Bullying
- Defamatory
- Disruptive
- Harmful to the school or local authority
- Harassing
- Insulting
- Intolerant
- Obscene
- Offensive
- Politically biased
- Threatening

Staff Email

All email messages should include a standard disclaimer stating that the content of the email are not necessarily the views of school or the Local Authority. Staff should not release or in any way make available personal details of any colleague or pupil (phone numbers, fax numbers or personal e-mail addresses) over the internet or through emails. The school complies with the privacy requirements of GDPR. When pupil personal data is transferred e.g. secondary schools, with permission from Headteacher and it is always password protected.

The sending of emails that are wholly or substantially unrelated to school business should be restricted to out of hours and designated breaks, and not completed using a school email account. All digital communications with parents/carers should be on a professional level and communicated via the school office not directly.

The sending of emails that are wholly or substantially unrelated to school business should be restricted to out of hours and designated breaks, and not completed using a school email account. All digital communications with parents/carers should be professional in tone and manner and communicated via the school office not directly. There is an understanding that any use of the school email system will be monitored and checked.

Communication between staff or members of the wider school community should be professional and related to school matters only.

Emails sent to external organisations will be written carefully and if necessary, authorised before sending to protect myself. As and when it is felt necessary, the headteacher, line manager or suitable member of staff may be carbon copied (cc) into the email.
Staff ensure that they manage their email accounts and delete emails no longer required. Information that they have a legitimate need to retain will not be kept in their email inbox but will be saved appropriately in the school's Sharepoint or OneDrive, ensuring access for other users if appropriate.
They will access their school email account on a regular basis to ensure that they respond in a timely manner to communications that require their attention.

Any personal device used to access school email or other communication systems will be encrypted and secured using a password in line with the school's password policy or biometric technology.
They will take care in opening any attachments sent by email. They will only open emails and associated attachments from trusted senders.

H) Images of children

Written permission from parents or carers is obtained for the following locations before photographs of pupils are published:

- On the school website
- In the school prospectus and other printed promotional material, e.g. newspapers
- In display material that may be used around the school
- In display material that may be used off site
- Parents and carers may withdraw permission, in writing, at any time.

This will be done on entry to the school and reviewed. A record of children with/without permission for images is held in the school office and on the pupil's Arbor. We do as a school, however, avoid using photographs of pupils for safeguarding purposes and may use backs of heads etc where possible.

Pupils and staff will only use school equipment to create digital images, video and sound involving children. In particular, digital images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online.

Staff may take digital images of children on a school device on a residential or sporting trip, where uploading images and tweeting are a means of communicating with parents.

Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites. All adults attending events have to sign to state that they agree to the above. Parents who attend as volunteers on school trips will be asked not to take photographs.

When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Any images, videos or sound clips of pupils must be stored on the school cloud system and never transferred to personally-owned equipment. When staff are accessing the remote desktop from personally owned machine, they're prohibited from downloading such material to their own device.

I) Social Networking

Staff and children are not allowed to use their personal account on social networking sites, such as FaceBook, MySpace or Bebo in school or on school machines unless they have been given permission by Senior Leaders. If staff have social networking accounts we recommend that their profiles are set to private. Staff must not have contact with children from our school through social networking sites, other than through the Learning Platform.

This is part of the Code of Conduct Policy:

SECTION 8: Social Contact and Social Networking

8.1. Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, tablets, text messages, emails, instant messages, websites, social media such as Facebook, Twitter, Instagram, chat-rooms, forums, blogs, apps such as Whatsapp, gaming sites, digital cameras, videos, webcams and other handheld devices. Adults should not share any personal information with pupils and they should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. They should ensure that all communications are transparent and avoid any communication that could be interpreted as 'grooming behaviour'.

8.2. Adults must not give their personal contact details such as home/mobile phone number; home or personal e-mail address or social networking details to pupils unless the need to do so is agreed in writing with senior management. If, for example, a pupil attempts to locate an adult's personal contact details and attempts to contact or correspond with them, the adult should not respond and must report the matter to their manager.

8.3. It is recommended that adults ensure that all possible privacy settings are activated to prevent pupils from making contact on personal profiles and to prevent pupils from accessing photo albums or other personal information which may appear on social networking sites.

8.4. Adults are personally responsible for what they communicate in social media and must bear in mind that what is published might be read by us, pupils, parents and carers, the general public, future employers and friends and family in perpetuity. Adults must ensure that their online profiles are consistent with the professional image expected by the school and must not post material which damages the reputation of the School or which causes concern about their suitability to work with children and young people. Those who post material which may be considered as inappropriate could render themselves vulnerable to criticism or, in the case of an employee, allegations of misconduct which may be dealt with under the disciplinary procedure. Even where it is made clear

that the writer's views on such topics do not represent those of the School, such comments are inappropriate.

8.5. *Adults are advised not to have any online friendships with any young people under the age of 18 unless they are family members or close family friends. Adults are advised not to have online friendships with parents or carers of pupils or members of the Governing Body/Trustees. Where such online friendships exist, adults must ensure appropriate professional boundaries are maintained.*

8.6. *It is acknowledged that adults may have genuine friendships and social contact with parents or carers of pupils, independent of the professional relationship. Adults should, however:*

- *Inform senior management of any relationship with a parent/carer where this extends beyond the usual parent/carer/professional relationship*
- *Advise senior management of any regular social contact they have with a pupil or parent/carer, which could give rise to concern*
- *Inform senior management of any requests or arrangements where parents/carers wish to use their services outside of the workplace e.g. babysitting, tutoring*
- *Always approve any planned social contact with pupils or parents/carers with senior colleagues, for example, when it is part of a reward scheme*
- *If a parent/carer seeks to establish social contact, or if this occurs coincidentally, the adult should exercise their professional judgment and should ensure that all communications are transparent and open to scrutiny.*

8.7. *Some employees may, as part of their professional role, be required to support a parent or carer. If that person comes to depend upon the employee or seeks support outside of their professional role this should be discussed with senior management and, where necessary, referrals made to the appropriate support agency.*

Staff should not post or make comments on social networking sites that may be interpreted as negative or harmful to the school, its employees, children or the local authority. Staff must follow the Code of Conduct in regards to their use of the internet.

E2BN guidance on using Facebook safely, as a school employee, can be found here:
http://www.e2bn.org/files/YHGfL_Guide_to_Using_Facebook_Safely2010.pdf

Face book provides support and advice for 'Educators' using Facebook:
http://www.facebook.com/help/?safety=educators

J) Mobile Phones, Smart watches and other digital devices

Ordinarily staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Staff must use a school phone where contact with pupils, parents or carers is necessary, unless there is a requirement for all staff to make contact with parents, for example, during times of remote learning. In these cases, staff will prevent their phone number from being disclosed.

Staff Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

The recording, taking and sharing of images, video and audio on **any** device (including watches) is to be avoided; except where it has been explicitly agreed otherwise by the Online Safety Lead. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary. All videos should be removed from the device as soon as possible and disposed of securely at the end of the period of work. Staff devices should use encryption and advanced password where available.

Where staff members are required to use a mobile phone for school duties, for instance in case of an emergency during off-site activities, they can use their own devices if they 'withhold' their own mobile numbers for confidentiality purposes. This is done by preceding the telephone number with the digits 141 before calling, e.g. 14101733123456. This will prevent the caller's number being displayed on the receiving phone.

Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

Personal mobile devices should NEVER automatically synchronise with any school endorsed system (except email), particularly where images from personal devices can be uploaded to school network spaces (such as Dropbox, RM Portico etc.)

The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.

We recommend that pupils should not bring mobile phones or personally-owned devices into school. It is only permissible for pupils in Years 5 and 6 to bring their mobile phones to school. Mobile phones belonging to children should be given to the office or locked in the class teacher's filing cabinet for safe keeping. Mobile phones will be returned at the end of the school day. The mobile phones will remain switched off until the child has left the classroom. The school takes no responsibility for personally owned devices brought into school.

We recommend that children do not wear smart watches or other devices. Smart watches should not be used for communication whilst in school or for video or photo use. The school takes no responsibility for any loss or damage that occurs on school premises.

K) Internet Games

There are times in the week when children have 'free' use of the school network, such as during computer clubs, wet playtimes, reward time for good behaviour etc. However, this access is still supervised by an adult. Any games played on the school network must be in line with the school rules and be suitable for primary aged children.

L) Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

M) Accessing Music and Films

Children should not download music onto the school network. If music is free to download it is usually illegal. Staff may download music, but this must be done legally, in line with copyright laws and for use within school e.g. from the Sing-up website and can only be completed by a 'Power User'.

The use of Spotify, Netflix and other subscription-based streaming services are allowed to be used with prior consent from the Headteacher. All usage will be age appropriate and abide by previously stated guidelines under Internet Use. For films which are rated PG and above prior consent from parents is required.

N) Filtering and Monitoring

The school uses a package recommended by The ICT Service (NetSweeper) on the network which filters and monitors the use of ICT. This software will:

- Log all computer activity to a central database

- Monitor and record an unlimited number of screens in real-time
- View current and previously opened windows, websites, applications, printed documents and deleted files
- Detect written keywords or sentences with screenshot or video evidence
- View evidence of attempts to access banned windows, websites and applications
- Instantly alert you of violations such as attempts to access banned websites
- Perform a number of operations such as logoff or send email upon violation detection

Netsweeper reports to members of SLT with daily alerts (when necessary) and weekly reports.

O) Sanctions

Sanctions will be levelled to the seriousness of the offence. For example, temporary suspension of ICT rights for minor offences, ranging to permanent exclusion, disciplinary action and involvement of the police for illegal actions.

P) School website

Any work published on the school website is thoroughly checked to ensure that there is no content that compromises the safety of pupils or staff. The school obtains parental permission before using images of pupils. We ensure the image file is appropriately named – we do not use pupils' names in image file names or ALT tags (Alt tags are the labels that describe the images on a website) if published on the web. This reduces the risk of inappropriate, unsolicited attention from people outside school. We will use group photos rather than photos of individual children, wherever possible.

Q) Curriculum Cloud System

The children will use generic whole class logons and user names. All adults have individual logon and passwords. User names and passwords must be kept secret and not shared with other users. All accounts are monitored through the online filters. If an adult forgets their username or password, this can only be reset by Lisa Dennis, School Business Manager. Supply teachers have a generic username and password which is changed regularly.

Filters are set differently for students and teachers to allow appropriate access.

Staff are able to save work through either the staffshare, my documents or on the cloud in Sharepoint or OneDrive. My documents/OneDrive are held under the individual account.

Teachers should follow the national curriculum for Computing. When teaching the National Curriculum, teachers should ensure that iPads are used for educational applications (apps) and not only for browsing the internet. Where research lessons are conducted on iPads, children

should complete this through safe browsers (e.g. Kiddle, Kidrex). Where more thorough research is needed, children should log in to a computer/laptop. Children should always be supervised whilst using iPads.

R) **Use of Artificial Intelligence (AI)**

The school recognises the growing role of artificial intelligence (AI) tools in education and expects all users to use them responsibly, safely and ethically. Staff may use the AI tool: CoPilot (that has had a DPIA agreed) to support learning, creativity and administrative tasks where appropriate; however, AI must not be used to generate work that is presented as a staff or pupil's own.

Users must not enter personal, sensitive or confidential information (including pupil data) into AI systems that are not approved by the school. All AI-generated content should be reviewed for accuracy, bias and suitability. Staff remain responsible for all decisions made using AI-supported information and must ensure outputs align with safeguarding, curriculum expectations and school values.
If personal and/or sensitive data is entered into an unauthorised generative AI tool, Fordham CE Primary School will treat this as a data breach and will follow the personal data breach procedure outlined in Data Protection Policy.

For more information on AI in schools please refer to the following guidance: **Generative artificial intelligence (AI) in education - GOV.UK** and **Guidance on AI and data protection | ICO**

S) Monitoring

The Headteacher and Online Safety Lead are responsible for monitoring and reviewing this policy every three years.

Child Protection Statement

At Fordham CE Primary School the welfare of the child is paramount. All children, whatever their age, culture, disability, gender, language, racial origin, religious beliefs and sexual identity have the right to protection from abuse. All suspicions and allegations of abuse and poor practice will be taken seriously and responded to without delay and appropriately. All staff and volunteers in school have a responsibility to report any concerns to one of the designated child protection officers.

Equalities Impact Statement:

1. *Has this policy fully considered the School's Equality objectives and statement?* ***Yes***
2. *Are there any impacts of the School's Equality objectives and statement on this policy?* ***No***
3. *If "Yes" are these clearly described and their impact assessed within the policy document?* ***N/A***

Appendix one

Reporting and dealing with incidents

Incidents of concern must be reported to the Online Safety Lead/Headteacher. A record of concerns is kept securely in the Headteacher's office.

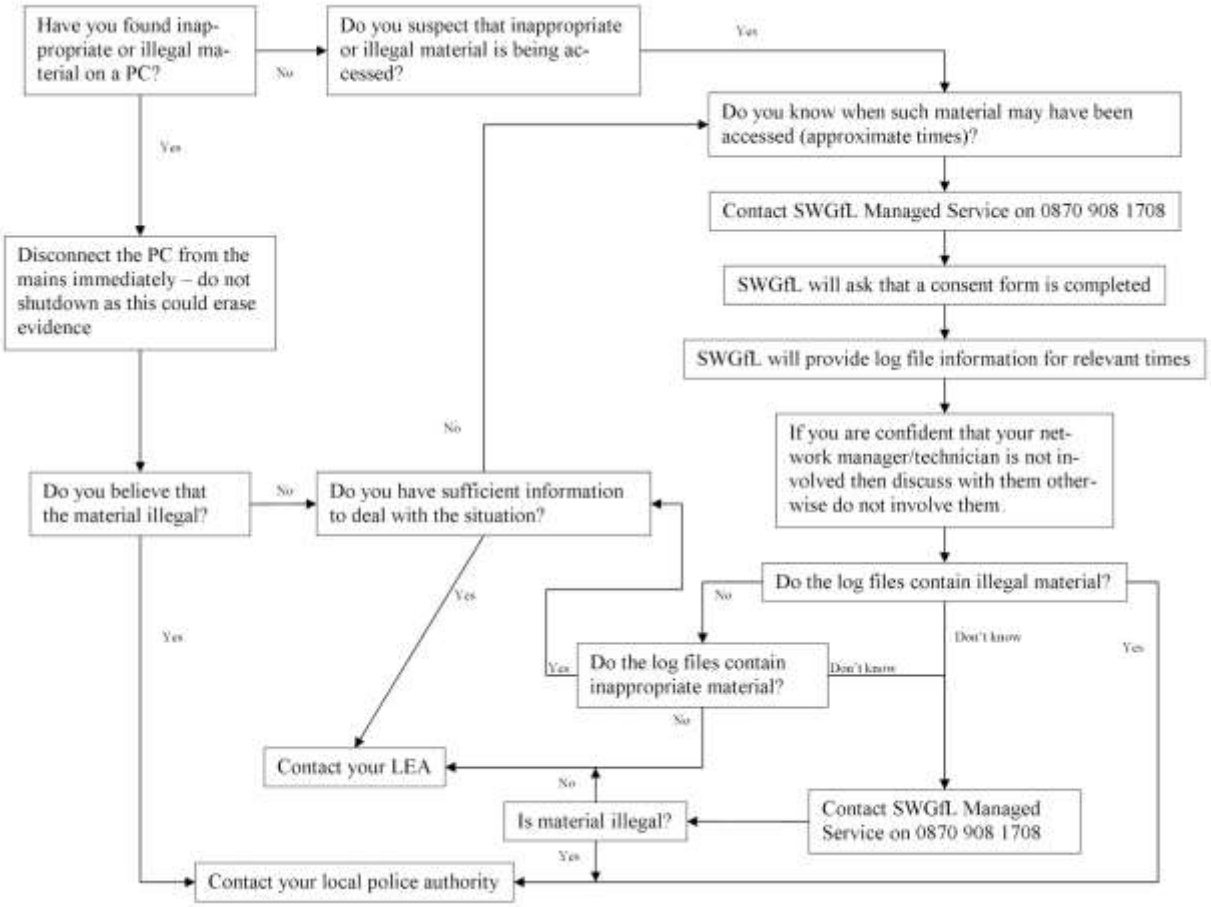
Any concern regarding children's safety to the Designated Safeguarding Lead.

If you find inappropriate or illegal material on a PC or other electronic device in school, do not try to capture or copy evidence, this may leave you in the position of distributing illegal images. Ensure children cannot access the inappropriate or illegal material - turn off the screen, remove the device to a secure place or switch off power at the wall. You then MUST report this to the Online Safety coordinator and Headteacher.

Dependent on the nature of the incident, we would either report concerns to the ICT Service or our Data Protection Officer. Governors would also be informed.

This flow chart is produced by South West Grid for Learning. It will be used as a guide for senior managers on how to deal with any incident.

Please note: our contact is The ICT Service, telephone 0300 300 0000, not SWGfL as on the flowchart.


Have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Do you know when such material may have been accessed (approximate times)?
Contact SWGfL Managed Service on 0870 908 1708
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them.
Do the log files contain illegal material?
No
Don't know
Yes
Do the log files contain inappropriate material?
Yes
Don't know
No
Yes
Disconnect the PC from the mains immediately – do not shutdown as this could erase evidence
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
No
Yes
Yes
Contact your LEA
No
Is material illegal?
Contact SWGfL Managed Service on 0870 908 1708
Yes
Contact your local police authority

Appendix two

KS2 Acceptable Use Policy

- I will use the school's ICT equipment and tools for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.
- I will keep my passwords private and tell an adult if I think someone else knows them.
- I will only use the internet when an adult is nearby.
- I will stay safe and I will not give my own personal details such as surname, phone number or home address or any other personal details that could be used to identify me, my friends, my school or my family (including wearing school uniform). If I have to use an online name, I will make one up!
- I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.
- I will never arrange to meet someone I have only ever previously met online. It could be dangerous.
- I will not deliberately look for, save or send anything that could be unpleasant or upsetting. If I find anything via Internet, e-mail or mobile phone that is upsetting or makes me feel uncomfortable, I will tell a teacher or responsible adult.
- I will only access my own documents and internet sites that teachers allow.
- I must not access or use AI tools independently at home or in school as I know it is not permitted to be used by pupils under the age of 13.
- I must not use AI to complete schoolwork or homework.
- I must tell a trusted adult if I encounter AI tools or are unsure about something online.

I will do my best to follow these rules because I know they are there to keep me and my friends safe.

If I don't follow these rules, my teacher may:

- Speak to me about my behaviour.
- Speak to my parents about my use of technology.
- Remove me from online communities or groups.
- Turn off my access for a little while.
- Not allow me access to use laptops / iPADs/ computers to access the internet or particular programmes.
- Take other action to keep me (and others) safe.

Appendix three

KS1 Acceptable Use Policy

- I will use the school's ICT equipment and tools (including computers, cameras etc.) for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.
- I will only use the internet when an adult is nearby.
- I will not share my passwords with other people and will tell my teacher if I think someone else knows them.
- I will stay safe and will not tell anyone online about myself or my friends (this is my name, home, family, pets or school address, school name etc.).
- I will care for and respect other people including online.
- I will ask my teacher or parent before using or uploading photos or video.
- If I see something on a screen, which upsets me, I will always tell an adult.
- I will remember that not everything on the internet is true.
- I will only connect with people who I know.
- I will not bring a mobile phone or digital recording device (e.g. smartwatch) to school.
- I must not access or use AI tools independently at home or in school as I know it is not permitted to be used by pupils under the age of 13.
- I must not use AI to complete schoolwork or homework.
- I must tell a trusted adult if I encounter AI tools or are unsure about something online.

I will do my best to follow these rules because I know they are there to keep me and my friends safe. If I don't follow these rules, I know that my teacher may stop me using technology at school and talk to my parents about how I use technology.

Appendix four

Parents, Visitors, Volunteers and Contractors Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of their professional responsibilities when using technology. This Acceptable Use of Technology Policy (AUP) will help Fordham ensure that all parents, visitors, volunteers and contractors understand the school's expectations regarding safe and responsible technology use.

I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all technology use is consistent with the school ethos, school staff behaviour and safeguarding policies, national and local education and children protection guidance, and the law.

Use of Mobile Devices and Smart Technology

Parents, visitors and contractors are respectfully requested not to use their mobile phones at all on the school site/in any area where children/young people are present.

- There is no available access to the school's internet unless it is agreed with the Headteacher.
- As a school, we filter the internet, restricting content that is available online and we monitor the use of the internet including sites visited and inappropriate searches. The reports generated record the time, which account and device has been used to access the highlighted content.
- Should phone calls and/or texts need to be taken or made, use is restricted to those areas not accessed by children and preferably off school premises to avoid any unnecessary disturbance or disruption to others.
- Should phone calls/and or texts need to be taken or made, visitors are asked to leave the premises to do so.
- Photos of children must not be taken without prior discussion with a member of the Senior Management Team and in accordance with the UK *General Data Protection Regulations (GDPR) and the Data Protection Act 2018* and using the 'Use of images consent form' (please refer to the school's document *"Guidance for schools and other establishments on the use of images"* 2022. Any individual bringing a personal device into the school must ensure that it contains no inappropriate or illegal content.
- Visitors to the school are requested to turn off their mobile phones at all times and adhere to the safeguarding requirements as agreed to on Inventry (the sign in device).
- As stated in Parents' Code of Conduct, we would like to discourage the use of mobile phones on school grounds particularly the use of cameras to avoid any misunderstanding and/or embarrassment. If we believe the camera application is being used whilst on school grounds, we may discuss this further with you. During school events, such as sports day, performances or in exhibitions of work, we ask that any photographs or videos taken on school site are for personal use **only** and not to be posted on social media.
- Adults either in school or accompanying children on school trips should not use their cameras or mobile phones cameras to take pictures of pupils. Adults, visitors or volunteers in school should only use their mobile phone within the confines of the school office or staff room. Personal cameras and

mobile phone cameras should not be used to take pictures of children. Parents accompanying children on school trips should not use their mobile cameras to take pictures of children.

Class Practice

- I will support teachers in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children I am supporting.
- I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content and if videos, images, text or music is protected, I will not copy, share, distribute or use it.

Safeguarding

- If I have any queries or question regarding safe and professional practise online either in school or off site, I will raise them with the Designating Safeguarding Lead or Lead for Online Safety.
- I will not upload, download or access any material which are illegal, such as child sexual abuse images, criminally racist material, adult pornography cover by the Obscene Publications Act.
- I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.
- I understand that if the school suspects criminal offences have occurred, the police will be informed.

Agreement

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

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

Name :
Role in School:
Signed
Date:
Accepted by:
Date:

APPENDIX E: Mobile Phone Agreement

Our Pupil Mobile Phone Rules

If you require your child to have a phone, then we recommend a phone without internet connectivity (a 'brick' phone) is brought into school.

- All pupils bringing a phone into school must have a good reason for doing so, and must have returned this agreement.
- All phones should be turned off when arriving on the school premises and handed in to the class teacher or the school office at the beginning of the day.
- Phones should be appropriately marked so that your child can recognise it with their name and class.
- Children should be reminded not to take photographs or videos of other children. This is because some children are not allowed to have their picture taken.
- Children should be reminded that access to the internet or messaging apps is not allowed whilst on the school premises.
- School cannot accept responsibility for damage to or loss of a mobile phone brought into school.
- No mobile phones are allowed to be taken on school trips – these should be handed in as usual practice or left at home. This includes on residential trips.

Parents will be contacted if children do not follow these rules. Any phone brought in without permission will be confiscated and parents or carers will be contacted.

Alongside parental responsibility for online safety, the school will help children to learn about staying safe online. The school will seek to work with families to help them to encourage children to adopt safe use of mobile technology.

Please note that there are certain apps that have age restrictions and therefore should not be used by the children.

Name of child ……

Class ……

Reason for needing a mobile phone in school: ……..

Parent / Carer: I confirm that I have explained the school rules regarding mobile phones to my child and can confirm that they may take a mobile phone into school on that basis.

Parent / Carer signature: …….. Date ……..

Pupil: I will follow the school mobile rules.

Pupil signature: …… Date ……..

PLEASE RETURN PERMISSION SLIP TO THE SCHOOL OFFICE OR CLASS TEACHER. THANK YOU.

……

APPENDIX 6: Declaration by staff

Please complete and return this page to the School Office.
As a staff member of the Fordham CE Primary School, I agree to comply with the rules, as explained within the Acceptable Use Policy.
Name:……
Signature:……
Date:……

Child Protection Statement

At Fordham CE Primary School the welfare of the child is paramount. All children, whatever their age, culture, disability, gender, language, racial origin, religious beliefs and sexual identity have the right to protection from abuse. All suspicions and allegations of abuse and poor practice will be taken seriously and responded to without delay and appropriately. All staff and volunteers in school have a responsibility to report any concerns to one of the designated child protection officers.

Equalities Impact Statement:

4. *Has this policy fully considered the School's Equality objectives and statement?* ***Yes***
5. *Are there any impacts of the School's Equality objectives and statement on this policy?* ***No***
6. *If "Yes" are these clearly described and their impact assessed within the policy document?* ***N/A***