



Saint Jérôme
Church of England
Bilingual School

Online Safety Policy

Policy created:	September 2024
Policy reviewed and updated:	September 2026
Date of next review:	September 2027
Review cycle:	Annually, by the Online Safety Co-ordinator, shared with the Governing Body at every review, supported by an annual online safety risk assessment.
Linked policies:	Child Protection and Safeguarding Policy, Behaviour for Flourishing Policy, Staff disciplinary procedures, Data Protection Policy and privacy notices, Complaints Policy.

Version history

Date	Version	Summary of changes
September 2024	V1	Original policy, based on the standard DfE/NSPCC model. Never signed off. The contents page listed five appendices, but only three were actually included: the two pupil-facing acceptable use agreements (EYFS/KS1 and KS2) and the staff training self-audit were promised but never drafted.
September 2026	V2	Drafted the three missing appendices: EYFS/KS1 and KS2 pupil acceptable use agreements (this is a primary school, so KS3/KS4 references have been removed), and a staff online safety training self-audit. Added a new section 4, Filtering and Monitoring, reflecting KCSIE 2026 paragraph 171, in force from 1 September 2026, which explicitly requires an annual effectiveness review led by a named senior leader, and connects filtering and monitoring to generative AI risk via DfE's 'Generative AI: product safety expectations' guidance; checked against current Harrow-area school policies, which all had a section of this kind that the 2024 version lacked. Added the UK Council for Internet Safety's 2024 update on AI-generated nude and semi-nude images (deepfakes), not covered in the 2024 version of this policy. Cross-referenced the current DfE Mobile Phones guidance and our Behaviour for Flourishing Policy's mobile phones section. Fixed a typo ('Intethernet' Safety). Updated governance titles and named individuals; the governor who oversees online safety could not be confirmed and is left as a placeholder.

Headteacher:

Kate Schutte

(Kate Schutte)

Co-Chairs of Governors: Approved by Governors on 17th September 2026

.....

(Vas Lappas and Edward Stowell)

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The Four Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- Content: being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact: being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images, including the consensual and non-consensual sharing of nudes and semi-nudes, and online bullying
- Commerce: risks such as online gambling, inappropriate advertising, phishing and financial scams.

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships Education, Relationships and Sex Education (RSE) and Health Education
- Searching, screening and confiscation
- Mobile phones in schools, which requires a mobile-phone-free school day by default; see section 9 and our Behaviour for Flourishing Policy
- The DfE's Filtering and Monitoring Standards for Schools and Colleges, and KCSIE 2026 paragraph 171, which requires an annual review of filtering and monitoring effectiveness; see section 4.

It also refers to the DfE's guidance on protecting children from radicalisation, and to the UK Council for Internet Safety's (UKCIS) Sharing nudes and semi-nudes: advice for education settings working with children and young people (2024 update), which now includes specific guidance on AI-generated nude and semi-nude images, sometimes called 'deepfakes'. This is an emerging risk that the 2024 version of this policy did not address.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, and the Equality Act 2010. It also reflects the Education Act 2011, which gives teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing the school's approach to safeguarding and related policies
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse, and some pupils with special educational needs and/or disabilities (SEND), recognising that a 'one size fits all' approach may not be appropriate for all children in all situations.

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our Child Protection and Safeguarding Policy, as well as relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Online Safety Co-ordinator in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with deputy DSLs, the Online Safety Co-ordinator and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Child Protection and Safeguarding Policy
- Ensuring that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the Behaviour for Flourishing Policy
- Ensuring updated staff training on online safety is delivered (Appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and external services if necessary
- Reviewing regular reports on online safety in school from the Online Safety Co-ordinator.

This list is not intended to be exhaustive.

3.4 The Online Safety Co-ordinator

The Online Safety Co-ordinator is responsible for:

- Ensuring an appropriate level of security protection, such as filtering and monitoring systems, reviewed and updated regularly to assess effectiveness and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Monitoring the school's ICT systems on a monthly basis
- Ensuring that access is blocked to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Behaviour for Flourishing Policy.

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy and implementing it consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3), and ensuring that pupils follow the school's terms on acceptable use (Appendices 1 and 2)
- Working with the DSL and Online Safety Co-ordinator to ensure that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Behaviour for Flourishing Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.6 Parents and Carers

Parents and carers are expected to notify a member of staff or the Headteacher of any concerns or queries regarding this policy. Parents and carers can seek further guidance on keeping children safe online from the UK Safer Internet Centre, Childnet International, and Disrespect Nobody.

3.7 Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Filtering and Monitoring

The Governing Body ensures the school has appropriate filtering and monitoring systems in place, covering the school's primary internet connection, any backup connection, guest Wi-Fi, and school-owned devices used off-site where possible. Our filtering provider is a member of the Internet Watch Foundation (IWF), so that known child sexual abuse material is blocked and cannot be overridden by school staff.

Our filtering and monitoring systems are provided by Crossover Solutions.

In line with KCSIE 2026, a named member of the Senior Leadership Team holds specific responsibility for filtering and monitoring.

The SLT lead for filtering and monitoring is Jack Corson, Assistant Headteacher, with oversight from Melanie Mckie.

This person, with support from the DSL and IT support, leads a review of the effectiveness of the school's filtering and monitoring systems at least once every academic year. This review considers whether the system blocks harmful and inappropriate content without unreasonably impacting teaching and learning; is up to date, operational, and applied to all users, school-owned devices, and devices using the school's broadband connection; and is age and ability appropriate. Evidence of each review, and any action taken as a result, is retained and made available to the Governing Body.

Where the school introduces a new generative AI tool for use by staff or pupils, this is treated as a trigger for an out-of-cycle review of filtering and monitoring arrangements, in line with the DfE's Generative AI: product safety expectations guidance, to check that the tool's risks are understood and that our filtering and monitoring systems can appropriately handle AI-generated content.

All staff are made aware of the school's filtering and monitoring systems and are expected to report any concerns about their effectiveness, including potential overblocking or underblocking, or ways pupils might bypass the systems, to the DSL or the SLT lead for filtering and monitoring without delay.

This section has regard to the DfE's Filtering and Monitoring Standards for Schools and Colleges.

5. Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the curriculum, drawing on the guidance on Relationships Education, RSE and Health Education.

In Key Stage 1, pupils will be taught to use technology safely and respectfully, keeping personal information private, and to identify where to go for help and support when they have concerns about content or contact online.

In Key Stage 2, pupils will be taught to use technology safely, respectfully and responsibly; recognise acceptable and unacceptable behaviour; and identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others, including in a digital context
- How to respond safely and appropriately to adults they may encounter, in all contexts including online, whom they do not know.

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse, and some pupils with SEND.

6. Educating Parents and Carers About Online Safety

The school will raise parents' and carers' awareness of internet safety in letters or other communications home, and in information via our website. Concerns or queries about this policy can be raised with any member of staff, the Headteacher, or the DSL.

7. Cyber-Bullying

7.1 Definition

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

7.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we ensure pupils understand what it is and what to do if they become aware of it happening to them or others, including knowing how to report incidents, whether they are a witness or a victim.

The school actively discusses cyber-bullying with pupils, explaining why it occurs, the forms it may take, and its consequences. Class teachers discuss cyber-bullying with their classes, and teaching staff are encouraged to find opportunities across the curriculum, including PSHE, to cover it.

All staff, governors and volunteers, where appropriate, receive training on cyber-bullying, its impact, and ways to support pupils, as part of safeguarding training (see section 12). The school also sends information and leaflets on cyber-bullying to parents and carers so they are aware of the signs, how to report it, and how to support affected children.

In relation to a specific incident of cyber-bullying, the school follows the processes set out in the Behaviour for Flourishing Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if necessary.

7.3 Examining Electronic Devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device they have reasonable grounds for suspecting poses a risk to staff or pupils, is identified in the school rules as a banned item for which a search can be carried out, or is evidence in relation to an offence.

Before a search, the authorised staff member will assess how urgent the search is and consider the risk to other pupils and staff; if it is not urgent, they will seek advice from the Headteacher. They will explain to the pupil why they are being searched, how the search will happen, give them the opportunity to ask questions, and seek the pupil's cooperation.

Authorised staff members may examine, and in exceptional circumstances erase, data or files on a confiscated device where they believe there is a 'good reason' to do so, meaning they reasonably suspect the device has been, or could be, used to cause harm, undermine the safe environment of the school or disrupt teaching, or commit an offence.

If inappropriate material is found, it is for the Headteacher to decide on a suitable response. If there are images, data or files that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response. If material may constitute evidence relating to a suspected offence, staff will not delete it, and the device will be handed to the police as soon as reasonably practicable. Otherwise, staff members may delete material if they reasonably suspect its continued existence is likely to cause harm to any person, or if the pupil or parent refuses to delete it themselves.

If a staff member suspects a device may contain an indecent image of a child, including an AI-generated nude or semi-nude image, they will not view the image, and will confiscate the device and report the incident to the DSL immediately, who will decide what to do next in line with the DfE's latest guidance on searching, screening and confiscation, and UKCIS guidance on sharing nudes and semi-nudes.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through our Complaints Policy.

8. Acceptable Use of the Internet in School

All staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors, where relevant, to ensure they comply with the above. More information is set out in the acceptable use agreements in Appendices 1, 2 and 3.

9. Pupils Using Mobile Devices in School

In line with current DfE guidance on mobile phones in schools, which requires a mobile-phone-free school day by default, pupil use and retention of mobile phones and other internet-enabled devices is not allowed in school. Pupils who need to carry a mobile phone to and from school will leave it, turned off, at the school office as soon as they arrive. See also the Mobile Phones section of our Behaviour for Flourishing Policy.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the Behaviour for Flourishing Policy, which may result in confiscation of the device.

10. Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure, including keeping the device password-protected with a strong password of at least 8 characters, combining upper and lower-case letters, numbers and special characters; making sure the device locks if left inactive; and not sharing the device among family or friends.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 3. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the Online Safety Co-ordinator.

11. How the School Will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour for Flourishing Policy and our teaching about using ICT safely. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the ICT usage agreement and staff code of conduct.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required, for example through emails, e-bulletins and staff meetings.

By way of this training, all staff will be made aware that technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse, including abusive, harassing and misogynistic messages; the non-consensual sharing of indecent nude and semi-nude images or videos, including AI-generated images; and sharing of abusive images and pornography with those who don't want to receive it. Training will also cover that physical abuse, sexual violence, and initiation or hazing-type violence can all contain an online element.

Training will help staff develop better awareness to spot the signs and symptoms of online abuse; develop pupils' ability to recognise dangers and risks in online activity and weigh them up; and develop the ability to influence pupils to make healthy long-term choices and stay safe from harm in the short term.

The DSL and deputy DSLs will undertake child protection and safeguarding training, including online safety, at least every 2 years. They, and the Online Safety Co-ordinator, will also update their knowledge and skills on online safety at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

13. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 5.

This policy will be reviewed every year by the Online Safety Co-ordinator. At every review, the policy will be shared with the Governing Body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online, since technology and its associated risks evolve and change rapidly.

14. Links with Other Policies

This policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour for Flourishing Policy
- Staff disciplinary procedures
- Data Protection Policy and privacy notices
- Complaints Policy
- ICT and internet acceptable use agreement
- Teaching of using ICT safely.

Appendix 1: EYFS and KS1 Acceptable Use Agreement

For pupils and parents/carers

I will:

- Ask a grown-up before I use the computer or tablet
- Only use the internet with a grown-up nearby
- Tell a grown-up straight away if I see something that makes me feel worried, sad, or uncomfortable
- Be kind to people online, just like I am kind in school
- Keep my name, address and password private, and not share them with anyone online
- Only click on things I know are safe, and ask a grown-up if I'm not sure.

Parent/carer agreement:

I have talked to my child about how to stay safe online, and I understand that the school will teach my child about online safety as part of their learning. I understand that the school may monitor my child's use of school ICT systems to help keep them safe.

Child's name: _____ Class: _____

Parent/carer name: _____ Signature: _____ Date: _____

Appendix 2: KS2 Acceptable Use Agreement

For pupils and parents/carers

When I am using school ICT systems and the internet, I will:

- Only use the internet and school systems for schoolwork, unless a teacher says it's okay to use them for something else
- Keep my passwords private and not share them with anyone else, including my friends
- Tell a teacher or trusted adult straight away if I see something online that upsets me, worries me, or that I think is inappropriate, even if it happens by accident
- Tell a teacher or trusted adult if someone online asks to meet me in person, asks for personal information or photos, or says something that makes me feel uncomfortable or unsafe
- Be respectful and kind to others online, and never send messages, images or comments that could upset, embarrass or hurt someone else
- Never share photos or videos of myself or other people, including friends and family, without checking with a trusted adult first
- Not use, or try to use, other people's accounts or devices without their permission
- Understand that anything I do on the school's ICT systems can be seen by staff, to help keep everyone safe
- Not bring personal devices, including mobile phones, into use during the school day, in line with the school's mobile phones rules.

Parent/carers agreement:

I have discussed the contents of this agreement with my child and understand that the school will provide guidance and education on online safety throughout the year. I understand that my child's use of school ICT systems may be monitored, and that the school will contact me if there are any concerns about my child's online safety or conduct.

Child's name: _____ Class: _____

Child's signature: _____ Date: _____

Parent/carers name: _____ Signature: _____ Date: _____

Appendix 3: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

Part A: All Staff, Volunteers and Visitors

All employees of Saint Jérôme Church of England Bilingual School have the opportunity to use the school's extensive ICT resources. To qualify to use these resources, all staff need to read and agree to the terms of this ICT user agreement.

The school strongly supports the use of ICT and every effort will be made to provide reliable resources to all users; however, inappropriate and/or illegal use of any ICT resource is strictly prohibited. If any user violates this agreement, access to ICT resources will be denied and the user may be subject to disciplinary action.

- **Personal Responsibility:** as a representative of the school, you accept personal responsibility for reporting misuse of ICT resources to a member of the SLT. Misuse includes any information sent, received or viewed that indicates or suggests pornography, unethical or illegal activities, racism, sexism, inappropriate language, or content likely to cause offence
- **Network Etiquette and Privacy:** be polite; use appropriate language; do not reveal personal information about yourself or others; remember email is not guaranteed to be private and may be screened; do not use ICT resources in a way that could disrupt others; respect the rights and beliefs of others
- **Services:** the school makes no guarantee of any kind for the ICT service provided and denies responsibility for the validity or accuracy of information obtained via its internet services. Data stored locally, such as on a laptop, is the individual user's responsibility to back up securely
- **Security:** report any security problem to the IT support provider, currently Crossover Solutions, at support@crossover.solutions, as soon as possible, without demonstrating the problem to another user. All use of ICT systems must be under your own username and password; sharing accounts or passwords may result in access being blocked
- **Vandalism:** any malicious attempt to harm or destroy equipment or data, including uploading or creating computer viruses, wilful damage to hardware, or deletion of data, is strictly prohibited
- **Electronic Mail and Messaging:** use only your official school email address to conduct school work; bulk sending of email without prior permission (spamming) is forbidden
- **Monitoring:** school email and system accounts are provided for the duration of your time at the school to undertake specific activities, and are not personal accounts. The school reserves the right to monitor activity using automated and manual methods
- **Disciplinary Consequences:** breaching this agreement may result in the removal of computer privileges, including logon, email and internet access, and may be reported to HR and the Senior Leadership Team for further action.

Part B: Workforce, Governors and Volunteers

The use of ICT resources must be in support of the role you perform for the school. You are personally responsible for this provision at all times when using any ICT resources. By using any school IT equipment after reading this agreement, you understand and accept the following terms:

- I will only use the school's email, internet, intranet and related technologies for professional purposes, or for uses deemed acceptable by the Headteacher or Governing Body
- I will comply with the ICT system security and not disclose passwords provided to me by the school or related authorities
- My passwords will be strong, including capitals, lower case, a number and a symbol, and at least 8 characters long; if I suspect a password has been compromised, I will change it immediately
- I will ensure I am the only person who uses my user account, and understand I am responsible for anything undertaken while logged in as me
- I will not autosave my password or login details for any school systems
- I will lock my computer screen whenever I leave it unattended
- I will ensure all electronic communications are compatible with my professional role
- If I receive a suspicious email, I will report it before clicking any links or entering my details, without forwarding the email, and instead send a screenshot

- My personal social media accounts will not show a direct link with the school; I understand my posts can be seen by others, so identifiable content will be professional in nature
- I will only use approved, secure email systems for school business, checking CC/BCC recipients, the correct address, and correct attachment each time
- I will ensure personal data is kept secure whether in the office or working remotely, and will store personal data on the school's Google Drive
- I will transfer personal data by email securely, for example using Egress or password protection, sending any password in a separate email
- I understand that anything I write about an identifiable person can be requested via a Subject Access Request and read by that individual
- I will not install hardware or software without the permission of the IT support provider
- I will consider whether communications I send breach confidentiality or data protection law before sending them
- I understand I can cause a data protection breach by destroying or corrupting data, and that data should be held in line with the school's data retention schedule
- I will not browse, download, upload or distribute material that could be considered offensive, illegal or discriminatory
- I will support the school's approach to online safety and will not upload images, video, sound or text linked to the school or its community onto my own social media
- I understand my use of the internet and related technologies can be monitored and logged, and made available on request to my line manager or the Senior Leadership Team
- I will respect copyright and intellectual property rights
- I will ensure my online activity, in and outside work, does not bring the school, my professional reputation, or that of others, into disrepute
- I will not use the school's ICT systems for commercial activities, such as work for a for-profit organisation.

Governors: Additional Guidance

Governors should familiarise themselves with the school's policies on acceptable use and e-safety, data protection, and breach management, and should be mindful of the seven principles of UK GDPR and the Data Protection Act: keep information secure; only store data for as long as needed or legally required; only use data required for the role; only use data for the purpose specified; ensure accuracy of data; handle data transparently; and be accountable, able to justify actions taken.

- Governing Body documentation is stored electronically on the shared portal, or securely in hard copy, in line with the school's Document Retention Policy. Information downloaded to a personal device should be deleted upon completion of the task
- School email addresses should be used for school business, and may be monitored where there is due cause
- When discussing business by email, individuals should be identified only as case reference numbers or initials where appropriate
- Deletion from an inbox does not mean an email cannot be recovered for disclosure purposes; treat all email as potentially retrievable
- Personal devices used for school business should have up-to-date anti-virus protection
- Attachments containing sensitive or confidential information should be encrypted so only the intended recipient can access them
- If an email is received in error, inform the sender and delete it, without using or disclosing any sensitive information it contains
- Any confirmed or potential data breach should be reported to the school without undue delay to allow the school to react and mitigate the impact.

User Declaration and Signature

I agree to abide by the ICT Policy and guidance. I understand that I have a responsibility for my own and others' online safety and undertake to be a safe and responsible digital technologies user. I understand it is my responsibility to stay up

to date and to read and understand the school's most recent online safety and safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: _____ Date: _____

Full name (printed): _____ Job title / role: _____

Authorised by (Headteacher), approving this user to be set up on relevant school systems:

Signature: _____ Date: _____

Appendix 4: Online Safety Training Needs Self-Audit for Staff

New for September 2026: this appendix was listed in the 2024 policy's contents page but never written.

To be completed by each member of staff annually, alongside safeguarding training, and passed to the DSL.

Name: _____ Role: _____ Date: _____

- I understand the four categories of online risk (content, contact, conduct, commerce) described in this policy: Yes / No / Not sure
- I know who the DSL and Online Safety Co-ordinator are, and how to contact them: Yes / No / Not sure
- I know how to log an online safety incident, and where the incident log is kept: Yes / No / Not sure
- I understand what to do, and what not to do, if I suspect a pupil's device contains an indecent image, including an AI-generated image: Yes / No / Not sure
- I understand the school's approach to examining and, where appropriate, confiscating pupils' electronic devices: Yes / No / Not sure
- I am confident recognising the signs that a pupil may be at risk of online abuse or exploitation: Yes / No / Not sure
- I understand my own responsibilities for acceptable use of school ICT systems, as set out in Appendix 3: Yes / No / Not sure
- I am aware of the school's current guidance on mobile phone use during the school day: Yes / No / Not sure
- I would find further training or support helpful on (please specify): _____

This form should be returned to the DSL, who will use it to identify whole-staff or individual training needs ahead of the next scheduled refresher training.

Appendix 5: Online Safety Incident Report Log

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident