

Online Safety Policy



Contents

Online Safety Policy.....	2
Aims.....	2
Legislation and guidance.....	2
Roles and responsibilities.....	3
Educating pupils about online safety.....	5
Educating parents about online safety.....	6
Cyber-bullying.....	7
Acceptable use of the internet in school.....	8
How the school will respond to issues of misuse.....	9
Training.....	10
Monitoring arrangements.....	10
Links with other policies.....	11
Appendix 1: EYFS and KS1 Pupil Online Safety agreement (pupils and parents/carers).....	12
Appendix 2: KS2 Pupil Online Safety Agreement (pupils and parents/carers).....	13
Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors).....	15
Appendix 4: Online safety training needs – self-audit for staff.....	16

Online Safety

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 4 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 (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and guidance

This policy is based on the Department for Education’s (DfE’s) statutory safeguarding guidance, Keeping Children Safe in Education (2024), and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Ensuring appropriate filtering and monitoring is in place

It also refers to the DfE’s guidance on protecting children from radicalisation.

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. In addition, it reflects the Education Act 2011, which has given 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.

Roles and responsibilities

The Board of Governors

The Eltham College Family of School's Board of Governors (ECFS) has overall responsibility for monitoring this policy and holding the Head to account for its implementation.

The Board of Governors allocated Safeguarding lead, 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) with the support of the IT Department.

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 services and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Head

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

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) is set out in our Child Protection Safeguarding Prevent policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head, Head of Digital Learning and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged 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 school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains an annual self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head and/or Board of Governors

This list is not intended to be exhaustive.

The IT Department

The IT Department is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this and any other applicable policy

The IT Department is supported by the academic Head of Digital Learning. The school also has an Online Safety Group.

This list is not intended to be exhaustive.

All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy 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 to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour 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.

Parents

Parents are expected to:

- Notify a member of staff or the Head of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online by visiting the Online Safety section of the Parent Portal. They are also provided with access to online support materials and training.

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be required to sign in using the school's digital sign-in system. During this process they 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 (appendix 3).

Educating pupils about online safety

Online safety is embedded within the school's safeguarding culture and curriculum. Pupils are taught about online safety through a planned, progressive programme within PSHE, Computing and the wider curriculum. This teaching reflects statutory requirements for Relationships Education and Health Education (primary), and is adapted to reflect emerging risks. *All* schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Recognise that people online may not be who they say they are
- Identify trusted adults and know how to ask for help if something online worries or upsets them
- Begin to understand how to behave kindly and respectfully online

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully, responsibly and securely
- Recognise acceptable and unacceptable behaviour online, including bullying and unkind communication
- Identify a range of ways to report concerns about content, contact or conduct
- Understand how information is shared online and the concept of a digital footprint
- Develop critical thinking skills to evaluate online content, including misinformation and AI-generated material

By the **end of primary school**, pupils will know:

- That people may behave differently online, including pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including respect, consent and boundaries
- How to recognise and respond to risks online, including harmful content, contact and conduct
- How to report concerns and seek support, understanding that all concerns will be taken seriously
- How to critically evaluate information and recognise unreliable, inappropriate or manipulated content (including emerging technologies such as AI-generated content)
- The risks associated with communicating with people they have not met in real life
- How personal data is collected, shared and used online
- What appropriate boundaries look like in online interactions with peers and adults
- How to respond safely to unknown or concerning contact, including from adults
- The potential impact of their online behaviour on themselves and others

Teaching about online safety is regularly reviewed and updated to reflect current risks and trends. Where necessary, provision is adapted to support vulnerable pupils, including those with SEND, recognising that a more personalised approach may be required.

Educating parents about online safety

The school recognises that parents and carers play a crucial role in supporting children to stay safe online. We are committed to working in partnership with families to promote a consistent and informed approach to online safety.

The school will proactively raise parents' awareness of online safety through:

- Regular communications (e.g. newsletters, emails and the parent portal)
- Guidance on emerging risks, including social media, gaming, and new technologies
- Information shared during parent evenings, workshops and meetings where appropriate
- Access to a curated library of online safety resources, including videos and guidance materials

The school will provide parents with clear and transparent information about:

- The systems used to filter and monitor online activity in school
- The types of online platforms, apps and websites pupils may be required to access
- How pupils may interact with staff or each other online for educational purposes
- The measures in place to safeguard pupils when using technology in school

We will also support parents to:

- Understand how to set appropriate parental controls and privacy settings
- Recognise signs that a child may be at risk online
- Respond confidently to online safety concerns at home

- Encourage safe, balanced and responsible use of technology

If parents have any concerns about online safety, they are encouraged to contact their child's Form Teacher or the Designated Safeguarding Lead (DSL) in the first instance. All concerns will be taken seriously and responded to in line with the school's safeguarding procedures

Cyber-bullying (online child-on-child abuse)

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying (child-on-child online abuse)

The school recognises that online abuse between pupils (often referred to as cyber-bullying) is a safeguarding issue and will be addressed accordingly.

To help prevent such behaviour, pupils are taught what online abuse is, why it occurs, and the impact it can have. They are supported to understand their responsibility to report concerns, whether they are directly affected or acting as a bystander.

Pupils are taught how to report concerns through multiple channels and are encouraged to do so in a safe and supportive environment.

Teaching about online abuse is delivered through PSHE, Computing and the wider curriculum. It includes:

- respectful online behaviour and communication
- consent and boundaries in digital interactions
- the risks associated with sharing content, including images
- the impact of harmful online behaviour on others

All staff, governors and volunteers receive training on recognising and responding to child-on-child abuse, including online abuse, as part of safeguarding training.

The school works in partnership with parents by providing guidance, resources and updates to help them recognise signs of online harm and support their children.

In response to incidents:

- All concerns will be taken seriously and considered from a safeguarding perspective
- Incidents will be recorded and reviewed to identify patterns or wider concerns
- The school will follow its behaviour policy where appropriate, alongside safeguarding procedures

Where illegal, harmful or inappropriate material has been shared, the school will take all reasonable steps to contain the incident and minimise further harm.

The Designated Safeguarding Lead (DSL) will take the lead in responding to safeguarding concerns and will refer cases to external agencies, including the police, where there are reasonable grounds to suspect a criminal offence.

Examining electronic devices

School staff have the power under the Education and Inspections Act 2006, as amended by the Education Act 2011, to search for and, where appropriate, delete data or files on pupils' electronic devices (including mobile phones and tablets) where there is a reasonable suspicion that the device contains material that may pose a risk to the pupil or others.

Any search will be carried out in a manner that is lawful, proportionate and respectful, having regard to the pupil's age, needs and individual circumstances.

When deciding whether there is a justifiable reason to examine or erase data or files on a device, staff must have reasonable grounds to suspect that the data or file has been, or could be, used to:

- Cause harm to the pupil or others
- Facilitate bullying, harassment or abuse (including online child-on-child abuse)
- Disrupt teaching and learning
- Breach school rules or policies

Where material is located on a device, staff will not act in isolation and will involve the Designated Safeguarding Lead (DSL) or a member of the senior leadership team as soon as possible. Decisions will be made on a case-by-case basis, taking into account safeguarding risk.

The school will determine whether to:

- Delete the material where appropriate and lawful to do so
- Retain the material as evidence of a potential safeguarding concern, breach of school rules or possible criminal offence
- Refer the matter to the DSL for further safeguarding action
- Report the matter to external agencies, including the police, where there are reasonable grounds to suspect a criminal offence

If a staff member has reason to believe that a device may contain a nude or semi-nude image, or any image that may be illegal to possess, they must not view the image. The device should be confiscated where appropriate and passed without delay to the DSL.

The DSL will decide on the appropriate course of action in line with:

- DfE guidance: Searching, Screening and Confiscation
- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings

All actions will be risk-assessed and focused on safeguarding, ensuring the welfare of the pupil remains the primary consideration.

Where there are reasonable grounds to suspect that a device contains evidence of a criminal offence, the device will be secured and handed to the police as soon as practicable.

All searching, screening and confiscation of devices will be carried out in accordance with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes

Any complaints regarding the searching or deletion of content will be managed through the school's complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are required to understand and adhere to the school's acceptable use agreements (appendices 1 to 3). Visitors will be expected to read and comply with these expectations where relevant.

Use of the school's IT systems and internet must be for educational purposes or in support of an individual's professional role.

The school uses appropriate filtering and monitoring systems to safeguard users and ensure compliance with this policy.

Further details are set out in the acceptable use agreements.

Pupils using mobile devices in school

The school recognises that personal devices can present safeguarding, privacy and wellbeing risks if not carefully managed.

Pupils in Year 4 and below must not bring electronic or Wi-Fi enabled devices (including e-book devices) into school.

Pupils in Years 5 and 6 may bring mobile phones and smart devices (including smartwatches) to and from school; however, all such devices must be handed in at the start of the day and stored securely until collection at the end of the day.

Pupils are not permitted to use mobile phones or smart devices on the school site.

The use of smart devices (e.g. smartwatches), which may enable communication, image capture or location tracking, presents additional safeguarding risks. These devices are therefore subject to the same controls as mobile phones and must not be worn or used during the school day.

Any use of mobile devices must comply with the school's acceptable use agreements.

A breach of these expectations may result in disciplinary action in line with the behaviour policy, including confiscation of the device. Safeguarding concerns will be referred to the DSL where appropriate.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- Using Two Factor Authentication where required;
- Ensuring that they only use school owned software and cloud services (*Unless actioning 2FA*);
- Making sure the device locks if left inactive for a period of time;
- Not sharing the device among family or friends;
- Installing security updates when prompted and reporting any potential issues as soon as possible.

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 and within the IT Equipment and Service Delivery and Online Safety policies.

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 IT Department.

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 policies on behaviour and ICT and internet acceptable use. 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 staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

Training

Online safety training is an integral part of the school's safeguarding strategy.

All new staff members receive training as part of their induction on:

- safe use of technology
- data protection and information security
- online safeguarding risks, including child-on-child abuse (sometimes referred to as cyber-bullying)
- the risks associated with online radicalisation

All staff receive regular updates and refresher training at least annually as part of safeguarding training, alongside ongoing updates through briefings, emails and staff meetings. This ensures staff remain aware of current and emerging risks.

Through this training, all staff are made aware that:

- Technology is a significant factor in many safeguarding and wellbeing concerns
- Children may be at risk of online abuse, exploitation and harm
- Online abuse can include:
 - abusive, threatening or misogynistic communication
 - non-consensual sharing of nude or semi-nude images and/or videos
 - exposure to unwanted or harmful content
- Harmful behaviours such as bullying, sexual harassment, coercion or violence may have an online element
- Emerging risks, including those linked to social media, gaming environments and AI-generated content, can increase safeguarding concerns

Training ensures that staff:

- Understand their safeguarding responsibilities and the role of the DSL
- Know how to recognise and respond to online safety concerns, including low-level concerns
- Are confident in reporting concerns in line with safeguarding procedures
- Understand the school's filtering and monitoring systems and their role in responding to alerts
- Are able to support pupils in developing safe and responsible online behaviours

The Designated Safeguarding Lead (DSL) and deputies undertake child protection and safeguarding training, including online safety, every 2 years in line with statutory guidance, and update their knowledge at least annually.

Governors receive appropriate safeguarding and online safety training to enable them to:

- Provide effective oversight and challenge
- Understand the school's approach to filtering, monitoring and online safety

Volunteers receive appropriate safeguarding and online safety information and training relevant to their role.

Further information about safeguarding training is set out in the school's Child Protection and Safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety via CPOMS.

This policy will be reviewed every year by the DSL and the nominated Data Protection Officer. At every review, the policy will be shared with the Board of Governors. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with other policies

This online safety policy is linked to our:

- Child Protection Safeguarding Prevent policy
- Behaviour policy
- Staff disciplinary procedures
- Complaints procedure
- IT Equipment and Service Delivery Policy
- Social Media Policy (Eltham Family of Schools)
- Privacy Notice (Eltham Family of Schools)
- Staff Privacy Notice (Eltham Family of Schools)
- Data Protection (Eltham Family of Schools)

Appendix 1: EYFS and KS1 Pupil Online Safety agreement (pupils and parents/carers)

The following information is shared with pupils via an online form. Pre-prep form is acknowledged as a class. The contents of the form will also be shared with Parents/Carers when requested

Acceptable use of the school's ICT systems and internet: EYFS and KS1 Pupils

Name of class:

When I use the school's computers and go on the internet, I will:

- Ask a teacher or adult before I use a computer or device
- Only go on websites that a teacher or adult has told me I can use
- Tell a teacher or adult straight away if:
 - I click on something by mistake
 - I see something that worries me or upsets me
 - I get a message from someone I don't know
- Be kind and polite to others when I am online
- Only use school computers for my learning
- Take care of the equipment and tell an adult if something is broken
- Keep my username and password safe and not share them with anyone
- Not share personal information (like my name, where I live or my school) without permission
- Save my work in the right place
- Check with a teacher before I print
- Log off or shut down when I have finished
- Tell an adult if anything online doesn't feel safe or right

I understand that the school can see the websites I use, and there will be consequences if I do not follow these rules.

Name of class and date of agreement recorded

Parent/carer agreement: I confirm that I give permission for my child to use the school's ICT systems and internet under the supervision of school staff. I acknowledge that I have read and understood the expectations for pupils' safe and responsible use of technology, as set out above, and I will support the school in ensuring that my child adheres to these expectations.

I recognise the importance of promoting safe and appropriate use of technology beyond the school environment and will raise any concerns relating to online safety with the school in a timely manner.

Distributed to parents for reference when requested

Accessed via an online form

Appendix 2: KS2 Pupil Online Safety Agreement (pupils and parents/carers)

The following information is shared with pupils via an online form. The contents of the form will also be shared with Parents/Carers when requested.

Acceptable use of the school's ICT systems and internet: KS2 Pupils

Name of pupil:

I will read and follow the rules in this acceptable use agreement.

When I use the school's ICT systems (such as computers) and access the internet, I will:

- Use the school's ICT systems responsibly and for educational purposes only
- Only use devices when a teacher is present or with their permission
- Keep my usernames and passwords secure and not share them with others
- Keep my personal information safe and not share details such as my name, address or contact information without permission from a teacher or parent/carer
- Tell a teacher or trusted adult immediately if I see or receive anything online that worries, upsets or confuses me
- Log off or shut down a device when I have finished using it
-

I understand that I must not:

- Access inappropriate websites or online services, including social networking, chat rooms or gaming sites, unless this is part of a supervised learning activity
- Open attachments, click links, or download files without checking with a teacher
- Use inappropriate, unkind or harmful language or behaviour online
- Create, share or post content that may be hurtful, inappropriate or unsafe, including images
- Use someone else's login details or allow others to use mine
- Arrange to meet anyone in person whom I have met online
-
- I understand that:
 - Online behaviour can have consequences for myself and others
 - Harmful behaviour online, including bullying or sharing content without permission, will be taken seriously
 - I should always report concerns, even if they seem small or involve someone else
 -
- If I bring a personal mobile phone or smart device (e.g. smart watch) into school:
 - I will hand it in at the start of the school day and collect it at the end of the day
 - I will not use it during the school day unless I have permission
 - I will use it responsibly and in line with school rules

Name of pupil and date of agreement recorded

Acceptable use of the school's ICT systems and internet: KS2 Pupils

I confirm that I give permission for my child to use the school's ICT systems and internet under the supervision of school staff. I acknowledge that I have read and understood the expectations for pupils' safe and responsible use of technology, as set out above, and I will support the school in ensuring that my child adheres to these expectations.

I recognise the importance of promoting safe and appropriate use of technology beyond the school environment and will raise any concerns relating to online safety with the school in a timely manner.

Distributed to parents for reference when requested

Appendix 3: Acceptable use agreement (staff, governors, volunteers and visitors)

The following information is shared with staff via an online summary.

Acceptable use of the school's ICT systems and internet: agreement for staff, governors, volunteers and visitors

This agreement ensures that all users understand their professional responsibilities when using the school's ICT systems and digital technologies. A digital version of this agreement will be provided to staff, governors and volunteers as part of induction and when a school device is issued.

Where IT equipment is issued (e.g. a Surface tablet), it is provided to support the fulfilment of professional duties. Devices may be taken off-site for school-related purposes; however, where they are required for day-to-day responsibilities, they must be available for use in school.

Further guidance should be read in conjunction with the school's IT Equipment and Service Delivery Policy. Any queries should be directed, in the first instance, to the IT Department.

I understand and agree that I will:

- Use the school's ICT systems and infrastructure for professional purposes only, in line with school policies
- Maintain the security of systems and data, including keeping passwords confidential and using multi-factor authentication where required
- Use only approved school systems and platforms for communication with pupils, parents and colleagues
- Maintain appropriate professional boundaries at all times, including not using personal email, messaging services or social media to communicate with pupils
- Not share personal contact details (e.g. mobile number, personal email) with pupils or parents
- Handle all personal and sensitive data securely and in accordance with data protection requirements, whether accessed on or off-site
- Report any concerns about data security, safeguarding or misuse of technology promptly in line with school procedures

I will also ensure that I:

- Do not install or use unauthorised software or hardware without permission from the IT Department
- Do not access, download, create or share material that is illegal, inappropriate or could cause harm or offence
- Use images of pupils and staff only for authorised purposes and in accordance with school policy; images must not be shared externally without appropriate consent
- Understand that all use of school systems may be monitored and logged, and accessed where necessary for safeguarding or management purposes
- Ensure that my use of technology, both within and outside school, does not negatively impact my professional role or bring the school into disrepute
- Act as a role model for safe and responsible use of technology and support pupils in developing good online safety behaviours

Safeguarding responsibilities

I understand that:

- Online safety is a safeguarding issue
- I must report any concerns about pupil safety, including online safety concerns and low-level concerns, to the Designated Safeguarding Lead (DSL) without delay
- I should not investigate safeguarding concerns independently but must follow the school's procedures

All users are required to read and acknowledge this agreement upon receipt of a school device or as part of their induction.

Further guidance is available via the Staff Homepage.

Appendix 4: Online safety training needs – self-audit for staff

The following information is shared with staff via an online form on an annual basis.

Online safety training needs audit	
Name of staff member/governor/volunteer/visitor and date of agreement recorded	
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	

Author/reviewer responsible:	Head of Digital Learning	ISI Document Code:	E-safety (Online) Policy 7h
Reviewed by:	DSL, Head	Date of last review:	May 2025
Authorised by resolution of:	Senior Leadership Team	Date of next review:	May 2025

Document version	Main Changes	Date	Who
Baseline	Rebranded the document	September 2022	IT Manager / IT Director
2022.1	Form links added to Pupil AUP's, Training Audit and Incident Reporting	December 2022	IT Director
2023.1	Revised wording for Section 7 – Pupil devices in School	January 2023	IT Director / SLT
2023.2	Review of wording to cover KCSIE 2023	September 2023	IT Director
2023.3	Policy name change to Online Safety Policy. Update to pupil agreement links	October 2023	Online Safety Group
2024.1	Annual review – Update to list of policies. Check of processes for filtering.	May 2024	IT Director / DSL / Head of Digital Learning
2025.1	Updated KCSIE to 2024. Updated Governors to ECFS. Removed reference to IT Manager. Update to Monitoring Arrangements	May 2025	DDDT
2026.1	Updated KCSIE to 2025 and RSE guidance. Reworded AUPs. Reference to smart watches more explicit. Removed Appendix 5.	May 2026	Head of Digital Learning
Distribution list	BP_Resources: Policies & Teacher_Resources School Website		