Online Safety Policy

Contents

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 (2023), 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 school's Board of Governors 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 Manager.

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 (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 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 Manager

The IT manager 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 (see appendix 5) and dealt with appropriately in line with this and any other applicable policy

The IT Manager is further supported by the Director of IT and the 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 (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 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

Pupils will be taught about online safety as part of their PSHCE and Computing lessons.

*All s*chools 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

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

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

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour

- 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. Further information can be found in the school's safeguarding policy.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating parents about online safety

The school will raise parents' awareness of internet safety in communications home, and in information posted on the school's parent portal.

Online safety advice will also be shared during parents' evenings and meetings where necessary. The school also provides parents with access to an online library of support videos.

The school will let parents know:

- What systems the school uses to filter and monitor online use

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Form Teacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff.

Cyber-bullying

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

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Discussions around cyber-bullying will take place during discrete ICT lessons and PSHE.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or

- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete the material, or

- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or

- Report it to the police**

- o If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

- o ** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 to 3). 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 to 3.

Pupils using mobile devices in school

For pupils in Year 4 and below, no electronic device or wi-fi enabled technology, including e-book devices should be brought into school. Pupils in years 5 and 6 are permitted to bring mobile phones to and from school on the understanding that they should be left in the designated storage location and collected at the end of the day. Children are not permitted to use mobile phones on the school site.

The wearing of smart devices, often connected to phones, poses potential safeguarding concerns and may result in the disruption of learning. For that reason, pupils in all year groups are not permitted to wear smart devices in school.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

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

All new staff members will receive in-person and online training, as part of their induction, on safe internet use, protecting data, 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.

- Children can abuse their peers online through:

    o Abusive, harassing, and misogynistic messages

    o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

    o Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

    o Training will also help staff:

    o develop better awareness to assist in spotting the signs and symptoms of online abuse

    o develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

    o develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include an element of online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and 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 Safeguarding Prevent policy.

Monitoring arrangements

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

This policy will be reviewed every year by the DSL and Clerk to the Board and Compliance 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 ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
    o I click on a website by mistake
    o I receive messages from people I don't know
    o I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
 	
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Name of class and date of agreement recorded
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.
Distributed to parents for reference when requested

Accessed via an online form: Click Here

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 the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Name of pupil and date of agreement recorded

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Distributed to parents for reference when requested

Accessed via an online form: Click Here

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

The following information is shared with staff via an online summary. Staff are also given access to the IT Service Delivery and Equipment and guidance on Protecting Information.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

This agreement is designed to ensure that all users are aware of their professional responsibilities when using any form of ICT. A digital overview of this information will be shared with staff, volunteers and governors when they are issued with a school device or as part of the induction process.

Where IT equipment is Issued (such as a Surface Tablet) it is to assist them in fulfilling their duties. This equipment may be taken home for school related business but where such equipment is required as an integral part of them being able to undertake their duties it must be available onsite every day.

Further reference should be made to the school's **IT Equipment and Service Delivery Policy** and any concerns or request for clarification should in the first instance be referred to the IT Manager or Director of IT.

- I acknowledge that I should only use the school's electronic infrastructure for professional purposes as defined in the **IT Equipment and Service Delivery Policy**.
- I acknowledge that I must comply with IT system security and not disclose any passwords provided to me.
- I must ensure that all electronic communications with pupils and staff comply with the **IT Equipment and Service Delivery Policy** and my professional role.
- I understand that I must not give out my own personal details, such as mobile phone number and personal email address, to pupils or parents.
- I understand that I can only use the approved, secure email system(s) for school business.
- I will ensure that personal or confidential data (such as data held on the school's MIS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without the express permission of the IT Manager so as to ensure compatibility and minimise the risk of viruses.
- I understand that I must not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy. Images will not be distributed outside the school network without the permission of the parent and Head.
- I understand that all my use of the Internet and other related technologies (including e-mail) can be monitored and logged and can be made available, on request, to the Head or designated person for child protection.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role or the school into disrepute.
- I will support and promote the school's **IT Equipment and Service** and help pupils to be safe and responsible in their use of ICT and related technologies.

All users are required to review and acknowledge this user agreement upon receipt of a school owned device. Further guidance and advice will be shared via the Staff Homepage: Device Acceptable Use Policy.

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?	

Accessed via an online form: https://forms.office.com/r/tdX2PpJnxP

Appendix 5: Online safety incident report log

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

Accessed via an online form: https://forms.office.com/r/URE7NkCHup

Author/reviewer responsible:	IT Director / IT Manager	ISI Document Code:	E-safety (Online) policy 7h
Reviewed by:	DSL, Head, IT Director, Head of Digital Learning	Date of last review:	July 2024
Authorised by resolution of:	Senior Leadership Team	Date of next review:	July 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
2024.4	Annual review – Update to list of policies. Check of processes for filtering.	May 2024	IT Director / DSL / Head of Digital Learning
Distribution list	BP_Resources: Policies & Teacher_Resources School Website		