



## Online Safety Policy

|                    |                           |                |
|--------------------|---------------------------|----------------|
| Reviewed by:       | Nurette Stanford - Bursar | August 2026    |
| Approved by:       | Trish Watt - Head         | September 2026 |
| Governor Approval: | Suzie Longstaff           |                |
| Next Review Date:  | September 2027            |                |

### Introduction

Online safety is an integral part of Eaton Square Prep School's safeguarding and child protection arrangements. The School recognises that technology is an important part of children's education and lives and is committed to ensuring that pupils are safeguarded from potentially harmful and inappropriate online material and activity.

This policy has been developed having regard to **Keeping Children Safe in Education (KCSIE) 2026**, the Department for Education's current guidance and standards on filtering and monitoring, and other relevant legislation and statutory guidance.

The School's approach to online safety is reflected in relevant policies and procedures, including the Safeguarding and Child Protection Policy, Acceptable Use Policy, Behaviour Policy and Anti-Bullying Policy, Staff Code of Conduct and Data Protection Policy.

All staff have a responsibility to safeguard pupils online. Any online safety concern which raises a safeguarding or child protection concern must be reported to the **Designated Safeguarding Lead (DSL), or a Deputy DSL in their absence**, and managed in accordance with the School's Safeguarding and Child Protection Policy.

The School will ensure that staff receive appropriate online safety information and training as part of safeguarding training and updates and understand their responsibilities in relation to the School's filtering and monitoring arrangements.

### Aims

The aims of this policy are to:

- safeguard and protect pupils from potentially harmful and inappropriate online material and activity;
- provide pupils with appropriate opportunities to use technology safely, responsibly and effectively as part of their education;
- ensure that pupils are taught, in an age-appropriate way, how to recognise, manage and report online risks and harms;
- ensure that staff understand their responsibilities for online safety and know how to identify, report and respond to online safeguarding concerns;
- maintain appropriate filtering and monitoring arrangements to help safeguard pupils when using the School's systems, networks and devices;
- promote a consistent whole-School approach to online safety involving pupils, staff, governors and parents; and
- ensure that the School's use of technology and online services is consistent with applicable safeguarding, data protection and other legal requirements.



In accordance with **Keeping Children Safe in Education (KCSIE) 2026**, the School recognises that online safety risks are broad and continually evolving and can be categorised into four areas:

- **Content** – being exposed to illegal, inappropriate or harmful content, including sexual or violent material, discriminatory content, self-harm or suicide content, radicalisation and extremism, misinformation, disinformation, conspiracy theories and harmful or inappropriate AI-generated content;
- **Contact** – being subjected to harmful online interaction with other users or technologies, including peer pressure, grooming, exploitation, inappropriate commercial contact and harmful interactions involving generative AI applications;
- **Conduct** – online behaviour that increases the likelihood of, or causes, harm, including online bullying, sharing personal information, making, sending or receiving explicit or intimate images, including AI-generated or manipulated images, and other harmful online behaviour; and
- **Commerce** – risks including online gambling, inappropriate advertising, phishing, scams and other forms of financial exploitation.

The School will take account of these four areas of risk in its safeguarding arrangements, online safety education, staff training, filtering and monitoring arrangements and engagement with parents.

## Internet Use

---

The purpose of Internet in School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management information and business administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet access is an entitlement for students who show a responsible and mature approach to its use.

The Internet is an essential element in the 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

### How will Internet use enhance learning?

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of the pupils. Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

### How will email be managed?

Eaton Square Prep. School encourages the use of email as an essential means of communication for both staff and pupils. Directed email can bring significant educational benefits and interesting projects between our school, and ones in other parts of the world can be beneficial.

School email accounts and systems are provided for School purposes and should not be considered private. The School may monitor the use of its email, network, devices and online systems where this is necessary and proportionate for safeguarding, security, regulatory compliance, the investigation of concerns or the effective operation of the School.



Any monitoring will be undertaken lawfully, proportionately and transparently in accordance with applicable data protection legislation, the School's Data Protection Policy and relevant Privacy Notices. Access to monitoring information will be restricted to appropriately authorised persons and information obtained through monitoring will be retained only for as long as necessary in accordance with the School's retention arrangements.

Where monitoring identifies a safeguarding concern, this will be reported to the DSL or a Deputy DSL and managed in accordance with the School's Safeguarding and Child Protection Policy.

Pupils are taught to email from Year 3 upwards. They are all allocated an individual email account, which is based on their first initial, surname and school domain. For example:

j.Smith@eatonsquareschools.com

Using this procedure, students maintain their anonymity outside the School.

All student email accounts from Years 3-6 have very strict restrictions attached. Year 2 have a whole class account.

- For all students the banned word threshold is 0, meaning that no inappropriate words can be used in any emails at all.
- Pupils in Years 3-5 are only allowed to email in class with teacher supervision.
- Pupils in Years 6 are also restricted to the eatonsquareschools.com. domain, but can have restrictions lifted in individual cases by the Head of ICT only. In this age group, pupils are taught how to access their email accounts from home and are encouraged to email their work/homework etc into their teachers.
- Pupils must immediately tell a teacher if they receive offensive email; this includes emails containing bullying in any form.

At all stages, the pupils are taught:

- the correct use of passwords and the importance of keeping them secret;
- appropriate use of language, formatting, formality and informality (depending on the purpose of the email)
- Internet and email safety – not giving out any personal information, such as address or telephone numbers, at any time to anyone; not arranging to meet anyone via email.

Pupils and staff will be informed, through appropriate policies and Privacy Notices, of the School's monitoring arrangements. Access to monitoring information will be limited to appropriately authorised persons. Any information arising from monitoring which indicates a safeguarding concern will be reported promptly to the DSL or a Deputy DSL.

Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

In a case where a pupil has sent an inappropriate email, the Head will decide on the course of action. In some cases, this may include suspension.

In a case where a staff member has sent an inappropriate email, the Head will decide on the course of action as set out in the Contracts of Employment.

Staff should not use personal email accounts during lesson times; access could be restricted if this occurs.



## Website Content

### How should website content be managed?

- The point of contact on the Website should be the School address, School email and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents will be obtained before photographs of pupils are published on the school website. Please see parent consent form.
- The Director of Marketing will take overall editorial responsibility and ensure that content is accurate and appropriate.

## Staff Social Media, Online Conduct and Professional Boundaries

All staff, governors, volunteers and other adults working on behalf of the School are expected to maintain appropriate professional standards and boundaries in their use of social media, messaging services and other online platforms, both in and outside School.

Staff must not use personal social media accounts, personal email addresses, personal telephone numbers or other personal online accounts to communicate with current pupils. Communication with pupils for School purposes must take place only through School-approved systems and in accordance with the School's policies and procedures.

Staff must not accept or initiate social media connections or friend/follow requests with current pupils.

Staff should exercise appropriate professional judgement in relation to online connections with former pupils and must ensure that professional boundaries are maintained at all times.

Staff must not use personal devices or personal accounts to take, store or share photographs, videos or other recordings of pupils for School purposes unless specifically authorised by the School and in accordance with the School's safeguarding, data protection and image-use arrangements.

Staff must not post, share or disclose confidential, sensitive or personal information relating to pupils, families, colleagues or the School. Staff must not post photographs, videos or other content relating to pupils or School activities through personal social media accounts.

Staff must not post or share content which is discriminatory, abusive, threatening, sexually inappropriate, defamatory or otherwise incompatible with their professional responsibilities or which may compromise the safeguarding of pupils.

Staff should take reasonable steps to protect their personal online security and privacy, including maintaining appropriate privacy and security settings, protecting personal contact information and being mindful that online content may be copied, shared or become publicly available regardless of intended privacy settings.

Staff should use their School email address and other School-approved communication systems for School business and should maintain an appropriate separation between their professional and personal online activity.



Staff must not use social media or online communications in a way which compromises professional boundaries with pupils or creates a safeguarding risk. Any concern about online contact or communication between a member of staff and a pupil must be reported in accordance with the School's Safeguarding and Child Protection Policy and Staff Code of Conduct.

Where a member of staff becomes aware of online content, contact or behaviour which raises a safeguarding concern about a pupil, they must report it immediately to the DSL or a Deputy DSL. Any concern or allegation about the online conduct of a member of staff, volunteer or other adult working with children must be reported and managed in accordance with the School's procedures for managing safeguarding concerns or allegations about adults working with children.

Staff who experience online bullying, harassment, threats, impersonation or other harmful online behaviour connected with their work should report the matter to an appropriate senior member of staff. The School will respond in accordance with its relevant policies and procedures and will provide appropriate support.

Breaches of these requirements may be dealt with under the School's disciplinary, safeguarding or other relevant procedures, as appropriate.

### Authorising Internet Access

Eaton Square Prep. School allocate Internet access to staff and pupils based on education need. All Internet usage by pupils is fully supervised at all times.

- Pupils in Key Stage 1 and Year 3 are restricted to using approved sites which have links provided by the teachers. Any general searching is very strictly monitored and at no time are the pupils allowed to search freely.
- In Years 4, 5 and 6, pupils can begin using approved search engines, under strict supervision, on their Microsoft Surface Go / Pro devices. They are taught to evaluate all content and to respect copyright regulations. The School's firewall has strict blocks in place, to limit the risk of children accessing websites with inappropriate content. Teachers can also monitor the student's devices through 'Classwize', allowing them to view the children's screens from their own device and block certain websites.

### Mobile Phones, Smart Devices and Mobile Data

The School is committed to maintaining a mobile phone-free environment throughout the School day in accordance with current Department for Education statutory guidance.

Pupils must not use mobile phones or other personal smart technology with similar functionality during the School day, including during lessons, breaktimes and lunchtimes, except where use has been specifically authorised by the School. Any arrangements for pupils bringing mobile phones or smart devices onto the School premises will be governed by the School's relevant policies and procedures.

Exceptions may be made where necessary to meet a pupil's individual needs, including where required as a reasonable adjustment for a disability or special educational need, or for medical purposes. Any exception must be agreed with the School and appropriately managed.

The School recognises that personal mobile phones, smart watches and other connected devices may access the internet through mobile data networks and may therefore bypass the School's filtering and monitoring systems. Pupils must not use personal mobile data, hotspots, tethering, VPNs or other technologies to circumvent the School's filtering, monitoring or security arrangements.



Where School-owned or School-managed devices are used, the School will ensure that appropriate filtering, monitoring and security arrangements are in place. The School will also consider the safeguarding implications of any personally owned device which is authorised for use on the School network or for educational purposes.

Any misuse of mobile phones, smart technology or mobile data which raises a safeguarding concern must be reported immediately to the DSL or a Deputy DSL and managed in accordance with the School's Safeguarding and Child Protection Policy. Other breaches will be managed in accordance with the School's Behaviour Policy and relevant Acceptable Use requirements.

Camera-enabled, audio-recording or AI-enabled smart glasses and similar wearable recording devices (including Meta/Ray-Ban smart glasses) are not permitted for use on the School site or during School activities by pupils, staff, parents, visitors or contractors. This restriction protects the safeguarding, privacy and personal data of pupils, staff and visitors and prevents unauthorised or covert recording. Exceptions for medical or accessibility purposes must be agreed in advance by the School.

## Filtering and Monitoring

The School recognises that appropriate filtering and monitoring systems are an important part of its safeguarding arrangements and maintains systems designed to protect pupils from illegal, inappropriate and potentially harmful online content and activity.

The Governing body, Dukes Education, has overall strategic responsibility for ensuring that appropriate filtering and monitoring systems are in place. The School will identify a **member of the Senior Leadership Team and a Governor** with responsibility for ensuring that the Department for Education's Filtering and Monitoring Core Standard is met.

The **Designated Safeguarding Lead (DSL)** has lead responsibility for safeguarding and online safety. The DSL will work closely with the Senior Leadership Team and the School's IT support to ensure that filtering and monitoring arrangements are effective. This will include reviewing relevant monitoring reports and alerts, responding to safeguarding concerns identified through monitoring and providing appropriate assurance to Governors.

The School uses appropriate technical filtering and monitoring systems, including **Smoothwall and Classwize**, to support its safeguarding arrangements. Filtering systems are designed to prevent access to illegal, inappropriate and potentially harmful content without unreasonably restricting teaching and learning. Monitoring systems support the identification of potentially concerning online activity so that appropriate safeguarding action can be taken.

Decisions about what content is blocked or permitted will be appropriately documented and will take account of the age and needs of pupils, safeguarding risks, curriculum requirements and the need to avoid unreasonable restrictions on teaching and learning.

Filtering and monitoring arrangements will be **reviewed at least annually** and whenever there is a significant change to the School's technology, systems or identified risks. The review will involve appropriate representatives from the Senior Leadership Team, the DSL, IT support and the responsible Governor. The review will consider the School's pupil risk profile, emerging online risks and the effectiveness and limitations of the systems in place.



Appropriate checks of filtering and monitoring systems will be undertaken and recorded during the academic year. The frequency and nature of these checks will reflect the School's context and identified risks. Checks will include relevant School-owned devices, services, user groups and School locations.

The School will ensure that filtering and monitoring arrangements are considered before new devices, systems, applications or online services are introduced for use by pupils. This will include consideration of technologies capable of providing dynamic or personalised content, including **generative artificial intelligence (AI)**.

All staff will receive appropriate information and training so that they understand their responsibilities in relation to filtering and monitoring, including how to report concerns and what action to take where potentially harmful or inappropriate online activity is identified.

Any online activity or monitoring alert which gives rise to a safeguarding concern will be reported to the DSL or a Deputy DSL and managed in accordance with the School's Safeguarding and Child Protection Policy.

Where staff or pupils identify a website or other online content which they believe should be blocked or reviewed, this should be reported through the School's established reporting arrangements so that appropriate action can be taken with the School's IT support and/or filtering provider.

Filtering and monitoring data will be accessed only by appropriately authorised persons and will be handled in accordance with applicable data protection legislation, including the UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025, the School's Data Protection Policy and relevant Privacy Notices.

## Generative Artificial Intelligence (AI)

The School recognises that generative artificial intelligence (AI) can provide educational and administrative benefits but may also present safeguarding, data protection, security, accuracy and intellectual property risks.

The use of generative AI by staff and pupils must be in accordance with the School's policies and procedures. Only AI tools approved by the School may be used for School purposes, and staff and pupils must comply with any age restrictions and terms of use applicable to those tools.

Where generative AI is made available to pupils, the School will consider the age and needs of pupils, the intended educational purpose, appropriate supervision and the safeguarding measures provided by the tool. Pupil-facing use will be subject to appropriate safeguards, including the School's filtering and monitoring arrangements.

Staff and pupils must not enter personal, confidential, special category or otherwise sensitive School information into generative AI tools unless the tool and proposed use have been specifically approved for that purpose and comply with the School's data protection arrangements.

AI-generated content must be treated critically and checked for accuracy, appropriateness, bias and reliability. Staff remain professionally responsible for any material they produce or use with the assistance of generative AI.

The School will consider the risks associated with generative AI as part of its online safety and filtering and monitoring reviews, including the ability of its systems to manage real-time, dynamic, personalised and AI-generated content.

Any use of generative AI which gives rise to a safeguarding concern must be reported immediately to the DSL or a Deputy DSL and managed in accordance with the School's Safeguarding and Child Protection Policy.

### How will the policy be introduced to the pupils?

Many pupils are familiar with Internet use and culture. Pupils' perceptions of the risks involved will vary so rules will need to be explained and discussed. Pupils may need to be reminded of the School rules at



the point of Internet use by referring to the Acceptable Internet and Computer Use Rules which are displayed in all rooms where computers are used, as well as in the Homework Diaries. A copy of the pupils' rules will be given to parents.

Pupils and staff will be informed that Internet use can be monitored and will be if necessary.

#### **How will the staff be consulted?**

It is important that teachers, learning support assistants, teaching assistants and administration staff are confident to use the Internet in their work. Staff should be given the opportunity to discuss issues and develop appropriate teaching strategies.

All staff must read the terms of the 'Acceptable Internet and Computer Use' statement, before using any Internet or computer resource in school.

Staff must be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff and pupils must understand the importance of maintaining security on the network. In this respect, staff and pupils must always log on under their own username, and at the end of a session must always log off.

No one is allowed access to another people's files unless given specific permission.

Staff should not knowingly delete any files other than their own. Deliberately deleting files belonging to the School or other individual teachers can result in action based on the Computer Misuse Act 1990.

### **How Will The ICT System Be Managed**

The School will maintain appropriate technical and organisational measures to protect its ICT systems, networks, devices and data from unauthorised access, loss, damage, misuse and cyber security threats.

The School will work with its IT support provider to ensure that ICT systems and devices are appropriately configured, maintained, monitored and supported, having regard to the Department for Education's current digital and technology standards, including the Cyber Security Core Standard.

The School will:

- ensure that operating systems, software, applications, devices and network infrastructure are supported and receive appropriate security updates and vulnerability fixes;
- maintain appropriate anti-malware, firewall and other security protections;
- control user access to systems and data according to role and need;
- require secure password practices and appropriate authentication, including multi-factor authentication where required or appropriate;
- ensure that privileged and administrative accounts are appropriately restricted, secured and managed;
- maintain appropriate backup and recovery arrangements for School systems and data;
- ensure that only authorised and appropriately approved software, applications, devices and online services are used for School purposes;
- restrict the use of removable storage media, including USB devices and external storage, to authorised circumstances and ensure that appropriate security measures are applied;
- maintain appropriate arrangements for securely connecting School-owned, personal and guest devices to the School's network;
- ensure that users do not attempt to disable, bypass or circumvent the School's security, filtering or monitoring arrangements; and



- regularly review cyber security risks and take appropriate action to address identified vulnerabilities.

Staff and pupils must use their own authorised accounts and must not share passwords or login credentials.

Users must take reasonable steps to prevent unauthorised access to their accounts and devices, including locking or logging out of devices when they are left unattended.

Any suspected cyber security incident, unauthorised access, loss of data, malware, phishing attempt or other security concern must be reported promptly in accordance with the School's established procedures. Where an incident gives rise to a safeguarding concern, it must also be reported immediately to the DSL or a Deputy DSL.

Cyber security incidents involving personal data will be managed in accordance with the School's Data Protection Policy and applicable data protection requirements.

## How Will Complaints About Internet/Computer Use Be Handled?

A clear process is in place for responding to concerns or incidents involving the use of the Internet, technology or School systems.

The School distinguishes between routine breaches of acceptable use or behaviour expectations and incidents which raise a safeguarding or child protection concern.

Any online incident or activity which raises a safeguarding or child protection concern must be reported immediately to the Designated Safeguarding Lead (DSL), or a Deputy DSL in their absence, and managed in accordance with the School's Safeguarding and Child Protection Policy.

This includes concerns arising from activity taking place both on and off the School premises where it may affect the safety or welfare of a pupil.

Safeguarding concerns may include, but are not limited to, online bullying or harassment; child-on-child abuse; grooming or exploitation; sexual harassment or sexual violence; the consensual or non-consensual sharing of nude or semi-nude images or videos, including AI-generated or manipulated images; exposure to harmful or illegal content; radicalisation or extremism; threats of harm; and any online activity which indicates that a pupil may be at risk of abuse, neglect or exploitation.

Pupils will be encouraged to report anything they encounter online which worries, frightens or upsets them and will be provided with clear, age-appropriate routes for doing so. Pupils will be reassured that concerns will be taken seriously and managed in accordance with the School's safeguarding procedures.

Where appropriate, online safety incidents which do not constitute safeguarding concerns may be managed in accordance with the School's Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, Staff Code of Conduct or disciplinary procedures, as applicable.

## Staff Misuse

A complaint about staff misuse may be referred to the Head.

Staff misuse can include, although is not exclusive to:

- Leaving a computer logged on after use.
- Accessing inappropriate websites.
- Accessing restricted files on the network.



- Deleting or altering other people's files without permission.
- Sending emails from the staff member's school account with inappropriate/illegal content.

If an incident has been reported to the Head, a variety of actions can take place as explained in the Staff Contract of Employment.

## Pupil Misuse

Where pupil misuse does not raise a safeguarding or child protection concern, it may be referred to the Head of ICT in the first instance and managed in accordance with the School's Behaviour Policy. Where the incident raises or may raise a safeguarding concern, it must be reported immediately to the DSL or a Deputy DSL.

### Child-on-Child Online Abuse

The School recognises that child-on-child abuse can take place online as well as face-to-face and that technology may facilitate or exacerbate abuse occurring between pupils. All staff must recognise that abuse can occur between children of any age and that the absence of a report does not mean that abuse is not taking place.

Child-on-child online abuse may include, but is not limited to:

- online bullying, including prejudice-based and discriminatory bullying;
- abusive, threatening, harassing or sexually inappropriate messages or communications;
- sexual harassment or sexual violence facilitated through technology;
- consensual and non-consensual making or sharing of nudes or semi-nudes, including AI-generated or digitally manipulated images;
- sharing photographs, videos or personal information without consent;
- coercion, exploitation, grooming or sexual extortion;
- deliberately excluding, humiliating or targeting another pupil online; and
- using social media, messaging, gaming platforms, AI or other technology to facilitate abuse.

Any concern about child-on-child online abuse must be reported immediately to the **DSL or a Deputy DSL** and managed in accordance with the School's Safeguarding and Child Protection Policy. Incidents will be considered on an individual basis, taking account of the age, development and circumstances of the pupils involved and any elements of coercion, exploitation or vulnerability.

Where an incident involves the making or sharing of nudes or semi-nudes, staff must **not view, copy, print, share, store or save the imagery, or ask a pupil to send or download it**. The matter must be referred immediately to the DSL or a Deputy DSL and managed in accordance with current safeguarding guidance.

Pupil misuse can also include, although is not exclusive to:

- Accessing the Internet without teacher permission and supervision
- Sending inappropriate emails
- Deliberately deleting files belonging to other pupils or teachers

If an incident has been reported to the Head of ICT, a variety of actions can take place based on the clearly established Behaviour Management Policy.

- The class teacher as part of the normal class discipline can deal with a minor transgression of the rules.
- Interview/counsel by the Head of ICT with a warning given.
- Informing parents.
- Referring to the Head or other senior management.
- Removal of computer/Internet access for a period, which could ultimately prevent access to files to complete school work.



- In extreme cases, a pupil can be suspended for a period of time determined by the Head.

**How will parents' support be enlisted?**

Parents' attention will be drawn to the School's Acceptable Use Policy in newsletters and the School website. A copy of the policy will be sent home annually when the parents are asked to sign the parental consent form.

It is important that parents are aware of the dangers of unrestricted access to the Internet and ways they can help their child at home. Internet issues must be handled sensitively to inform parents without undue alarm.

We encourage a partnership with parents. Suggestions are made to parents for safe Internet use at home. We aim to promote a consistent approach between the home and school.