EATON HOUSE SCHOOLS

ONLINE SAFETY

POLICY

Responsibility:	Mrs Roosha Sue (Head, EHTM Nursery) Mrs Claire Fildes (Head, EHTM Girls') Mrs Kirsten Bond (Head, EHTM Pre-Prep) Mr David Wingfield (Head, EHTM Prep) Mr Ross Montague (Head, EHB) Mrs Alison Fleming (Principal, Eaton House Schools) Mr Liam Corbett (Bursar, Eaton House Schools)
Reviewed:	August 2025
Current version no:	2025v1
Next review:	August 2026

Contents

Introduction

Eaton House School the Manor (EHTM) and Eaton House School Belgravia (EHB) are committed to ensuring the safety and well-being of every pupil in their care. The same safeguarding principles that apply in the physical world extend equally to the digital environment.

This policy applies to all members of the Eaton House community, including staff, students, parents and visitors, who have access to and/or are users of the Schools ICT systems, whether on or off the premises. In particular, this policy addresses the (mis)use of any of the above technologies, whether on or off School premises.

The internet and ICT offer valuable opportunities for learning and personal growth. However, they also come with risks, including cyberbullying, sexting, grooming, sexual exploitation, radicalisation, and data privacy breaches. These dangers can impact personal safety, mental and physical health, and relationships. Additionally, cybersecurity threats may compromise the integrity of the Schools ICT system. To address these risks, Eaton House Schools takes both technical and educational measures to ensure a safe and adaptable technology environment at the School.

The Schol has zero tolerance for abuse, including bullying, sexual harassment, violence, and discrimination. Students and staff should report any concerns, no matter how small, to a trusted staff member or the Designated Safeguarding Lead (DSL). The DSL will be informed of all concerns and take appropriate action with support provided.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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

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, extremism misinformation, disinformation (including fake news) and conspiracy theories.
- 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

Roles and Responsibilities

Principal and headteachers

The principal and headteachers have overall responsibility for monitoring this policy and ensuring its consistent implementation across Schools.

They will:

- Ensure staff undergo online safety training as part of child protection and safeguarding procedures.
- Clarify staff expectations, roles, and responsibilities regarding filtering and monitoring.
- Ensure that children are taught how to keep themselves and others safe, including online safety.
- Oversee regular online safety updates for staff (via email, e-bulletins, and staff meetings), at least annually, to maintain staff skills and knowledge in safeguarding children.
- Ensure the school has appropriate filtering and monitoring systems in place for school devices and networks, and regularly assess their effectiveness.
- Review the Department for Education (DfE)'s filtering and monitoring standards and discuss with the IT staff and service providers to ensure the school meets standards;

    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
    - Reviewing filtering and monitoring provisions at least annually;
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
    - Having effective monitoring strategies in place that meet their safeguarding needs.

The Designated Safeguarding Leads (DSLs)

Details of the School's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

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

- Supporting in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- To review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Ensuring that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- 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
- Providing regular safeguarding and child protection updates, including online safety, to all staff

The ICT Manager

The ICT Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security frequent check and monitoring the school's ICT systems
- 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 policy
- Assisting the Heads and DSLs on cyber-bullying incidents

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, and ensuring that pupils follow the School's terms on acceptable use
- 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'

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher 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

Parents/carers may seek further guidance on keeping children safe online from the following organisations:

- What are the issues? – UK Safer Internet Centre
- Online safety topics for parents/carers – Childnet
- Parent resource sheet – Childnet

Education and Curriculum

Computing plays a vital role in education. It is both an essential subject in the curriculum and a key tool for delivering high-quality learning experiences. At Eaton House Schools all classrooms are equipped with electronic whiteboards, projectors, and computers. Each school has an ICT suite, where students can access computers for private study under supervision.

While being online presents certain risks, Eaton House Schools acknowledges the significant opportunities and benefits it offers. Technology is deeply integrated into daily life, making it crucial for students to develop the skills to understand and use it effectively. These competencies are essential for their future success.

Key subjects for Online Safety integration

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing
- English

All staff have a responsibility to incorporate online safety across all aspects of school life. This includes embedding digital awareness into the curriculum, supporting subject leads, and making use of unplanned learning opportunities when they arise.

Technology use and monitoring

When overseeing the use of technology, whether in the classroom, for homework, or through emerging tools staff must promote responsible use. They should monitor student activity, assess potential risks, and ensure online resources are age-appropriate.

Parents and carers should be informed about the systems in place to filter and monitor online activity. They should also be made aware of their child's online learning tasks, the websites they will use, and any interactions with school staff in digital spaces. As outlined in Keeping Children Safe in Education (KCSIE) 2025, clear communication with parents is essential.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Cyber-bullying

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

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.

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.

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.

Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Microsoft Co Pilot and Google Gemini.

Eaton House Schools recognises that AI has many positive application in educationand can support teaching and learning. However it also acknowledges that AI presents safeguardingrisks particularly in the form of online harms. These include its potential misuse to bully others, for example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Eaton House School will treat any use of AI to bully pupils very seriously.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment, where possible for new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

In line with KCSIE 2025, Eaton House Schools acknowledges the Department for Education's guidance on Generative AI: product safety expectations, which outlines how filtering and monitoring requirements apply to AI use in education. The school will ensure that appropriate filtering and monitoring systems are in place to support the safe use of generative AI, in accordance with this guidance.

Pupil using mobile devices in School

Please see a separate pupil mobile phone policy.

Procedure

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 and 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safeguarding, including online safety.

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:
- Abusive, threatening, harassing and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- 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
- Training will also help staff:
- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

Monitoring arrangements

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

This policy will be reviewed annually.

Appendix A - Meeting Digital and Technology Standards at Eaton House Schools

Broadband Internet Standards

Eaton House Schools maintains a high-speed internet connection with a 100mb/s leased line provided by Babble. To ensure continuity, we have a backup FTTC connection with a speed of 70mb/s. Our firewall is equipped with an automatic failover system to seamlessly switch to the backup connection in case of primary network failure. Additionally, our network devices have short-term backup power supply options to mitigate disruptions during brief outages.

Security and Safeguarding

Our network security is reinforced by a Smoothwall firewall, which also includes built-in content filtering and monitoring. Internet activity is continuously monitored, with daily reports sent to Designated Safeguarding Leads (DSLs) and instant alerts triggered for specific categories of concern. However, we do not currently have measures in place to block VPNs and proxy services.

Network Switching Infrastructure

The School's network infrastructure is built using Aruba switches, which are not stackable, and they interconnect at a speed of 1Gb/s. Administrative access to these switches is managed securely by IT through password protection. We do not use a web-based platform for monitoring or managing our network switches.

Network Cabling Standards

Our network is wired with a combination of Cat 5e and Cat 6 cabling, with the most recent installation performed by InTouch. Cable testing is conducted as needed, and efforts are made to comply with British Standards (BS 6701, 50173, 50174). Network cables are separated from power cables where possible to minimise interference.

Wireless Network Standards

Eaton House Schools utilises WiFi 5 and WiFi 6 technologies for wireless connectivity, managed through a Unifi Cloud Key. Content is monitored via Smoothwall. While guest users are allowed on the network, staff and student networks are not yet separated. Security is ensured through WPA2 encryption.

Cybersecurity Standards

Our cybersecurity framework is based on CIS Controls v2.0. System access is managed via Active Directory and Microsoft 365, with multi-factor authentication (MFA) implemented for staff

accounts. Cybersecurity incidents and data breaches are handled through Dukes, with external support from Fresh Security. Additionally, all endpoints are protected using Sophos Intercept X anti-malware solutions.

Filtering and Monitoring

Internet safety is maintained through Smoothwall filtering and monitoring. Any flagged inappropriate activity is reported daily to DSLs, with immediate alerts issued for high-priority concerns. Filtering and monitoring policies undergo termly reviews to ensure effectiveness.

Cloud Solutions

We utilise Microsoft 365 for cloud storage and collaboration, with two-factor authentication (2FA) ensuring data security. Cloud data is stored in the UK and backed up to Barracuda. All data transfers are encrypted using 256-bit AES encryption.

Servers and Storage

The school operates three Hyper-V servers running approximately ten virtual machines, responsible for Active Directory, file and print services, DHCP, DNS, AB Tutor, and English Type. Backups occur nightly to the cloud via Barracuda, with data stored in the UK. The servers are equipped with redundant power supplies, UPS protection, and RAID configurations for data redundancy. They are housed in a secure, climate-controlled environment at the Manor.

Compliance and Data Protection

User accounts and access permissions are managed by the IT Manager. Personal and sensitive data are protected through access controls on folders and files to ensure data privacy and security.

Business Continuity and Disaster Recovery

In the event of a failure or attack, systems are restored to an unaffected site. The Bursar and IT Manager are responsible for coordinating disaster recovery efforts.