

Online Safety Policy

The Eden School



Approved by:

The Board of
Governors

Date: 31st of August 2024

Last reviewed on:

1st September 2025

Next review due by:

31st August 2026

Overview

At The Eden School, we are committed to ensuring the safety of our pupils, staff, volunteers, and the wider school community in the digital world. This policy outlines our approach to online safety and provides clear mechanisms to protect, educate, and manage online risks and incidents.

Aims

Our school aims to:

- Implement robust processes to safeguard pupils, staff, and the school community online.
 - Provide an effective approach to online safety, empowering individuals to use technology responsibly and securely, including mobile and smart devices.
 - Ensure clear procedures are in place to identify, manage, and escalate online safety concerns.
-

The 4 Key Categories of Risk

Our approach to online safety addresses the following risks:

1. **Content** – Exposure to illegal, harmful, or inappropriate material (e.g., pornography, hate speech, radicalisation).
 2. **Contact** – Harmful interaction with others online (e.g., grooming, exploitation).
 3. **Conduct** – Risky online behaviour (e.g., cyberbullying, sharing explicit images).
 4. **Commerce** – Risks such as online gambling, phishing, or financial scams.
-

Legislation and Guidance

This policy is based on:

- The Department for Education's (DfE) statutory safeguarding guidance, *Keeping Children Safe in Education (KCSiE)*.
 - *Teaching Online Safety in Schools* guidance.
 - *Cyberbullying: Advice for Headteachers and School Staff*.
 - The National Curriculum computing programmes of study.
-

Roles and Responsibilities

All staff, governors, volunteers, and pupils have a duty to use technology responsibly and report any concerns about inappropriate behaviour. We work together to promote a culture of safety and support within the school.

- **DSL (Designated Safeguarding Lead):** Oversees online safety concerns and incidents, ensuring proper protocols are followed.
- **Teachers and Staff:** Deliver online safety education and monitor online activities within the school environment.
- **Governors:** Receive training on online safety issues and monitor compliance with safeguarding responsibilities.
- **Parents:** Receive training and guidance to support safe technology use at home.

Education and Curriculum

We incorporate online safety education across the curriculum, promoting digital literacy and resilience from Early Years to Key Stage 5.

- **Key Stage 1** pupils learn to use technology safely and understand the importance of keeping personal information private.
- **Key Stage 2** pupils are taught about acceptable and unacceptable behaviour online, and how to report concerns.
- **Secondary School Pupils** receive age-appropriate online safety lessons, focusing on privacy, cyberbullying, and responsible use of social media.

Cyberbullying

Cyberbullying is defined as the use of technology to bully a person or group, involving a power imbalance. It is repetitive, intentional harm that may occur on social media, messaging apps, or online gaming platforms.

To prevent and address cyberbullying:

- **Education:** Pupils are taught about the effects of cyberbullying and how to report incidents.
- **Support:** We offer guidance to pupils and parents, and provide access to counselling services where necessary.
- **Discipline:** Incidents are managed in line with our behaviour policy and referred to the DSL if serious or illegal content is involved.

Parental Involvement

Parents are provided with resources and workshops to help them manage their children's online safety. These workshops include training on setting up parental controls, understanding online risks, and managing digital devices at home.

Handling Online Safety Concerns and Incidents

All online safety concerns should be reported to the **DSL** or headteacher, who will handle incidents according to safeguarding procedures. In severe cases, incidents may be escalated to external authorities, such as the local authority's safeguarding hub (MASH) or the police.

Misuse of School Technology

We maintain strict rules on the use of school devices, networks, and systems. Any misuse by pupils will be addressed in line with the school's behaviour policy, and staff are subject to disciplinary action under the staff code of conduct.

Appropriate Filtering and Monitoring

At The Eden School, we take a comprehensive approach to ensuring that all students and staff are safe when using digital tools, both in school and at home. Our online safety strategy is built on a combination of tools and systems that monitor, filter, and protect our digital learning environment.

1. **Google SafeSearch:**

- We use **Google SafeSearch** to block explicit and inappropriate content across our school's internet-enabled devices. SafeSearch is enforced on all browsers used in school, helping to ensure that searches, especially by younger students, return safe and educational results. This feature is also extended through Google-powered tools to monitor search activities for students.

2. **Google Extensions and Tools:**

- **Google extensions** such as **AdBlock** and **Safe Browsing** are used to add an extra layer of protection. These tools help prevent exposure to inappropriate content, phishing attacks, and intrusive ads.
- We also use **Google Family Link** on managed devices to control and filter what websites and apps students can access.

3. **Circle SafeSearch:**

- For our most vulnerable and difficult students, we have integrated **Circle SafeSearch**, which provides more granular control over internet usage and filters inappropriate content at a stricter level. This system allows real-time monitoring and reporting on the student's internet activity and enables us to block harmful content more effectively.

4. **Microsoft Teams:**

- Microsoft Teams is used as a core communication and collaboration platform for our students and staff. While Teams does not have built-in filtering for web content, we implement **Microsoft Defender** and **Safe Links** for added security. These tools help protect students from harmful links and malicious attachments within Teams communications.
- Additionally, **Microsoft 365 Compliance** tools are employed to track communication patterns and alert staff to potential safeguarding risks, such as cyberbullying or sharing of inappropriate content.

5. **Safe Internet Browsing Across Platforms:**

- Across all devices, we maintain strict filtering using **Google Safe Browsing** and **Microsoft's Safe Links** to scan and block access to malicious or inappropriate websites. Our policy includes monitoring tools like **Microsoft Defender** for real-time threat detection, ensuring that our students are protected against harmful content.

6. **Monitoring Tools:**

- **Google Safe Browsing API** is used to monitor websites visited across our network, automatically blocking malicious sites. For students identified as needing more intensive supervision, **Circle SafeSearch** provides heightened filtering and detailed activity reports to designated staff members.
- **Teams Compliance Monitoring** ensures that inappropriate messages or files shared within the platform are flagged for review by staff, enabling us to intervene when necessary.

Monitoring and Safeguarding

Our comprehensive approach ensures that online safety is maintained through both **Google** and **Microsoft** ecosystems, with enhanced support for vulnerable students using **Circle SafeSearch**. The IT department works closely with teaching staff to implement these tools and ensure their consistent

use. All filtering and monitoring systems are regularly updated, and staff receive ongoing training on their use.

In the event of a breach or an online safety incident, the **Designated Safeguarding Lead (DSL)** and the **IT Manager** are notified immediately, and appropriate action is taken to safeguard the individual(s) involved.

Device Usage and Personal Devices

- **Pupils:** Pupils are not allowed to bring mobile phones or personal devices to school unless permitted for a specific purpose (e.g., for a school trip).
 - **Staff:** Staff may use personal devices in non-contact times, but personal use must comply with the school's code of conduct.
 - **Parents and Visitors:** Parents and visitors are not permitted to use mobile phones while on school premises unless authorised.
-

Searching and Confiscation

The headteacher and authorised staff have the power to search and confiscate personal devices if there is reasonable suspicion of illegal or inappropriate material.

Appendices

- **Appendix 1:** Online Safety Rules for Pupils.
 - **Appendix 2:** Acceptable Use Agreement for Staff, Governors, Volunteers, and Visitors.
 - **Appendix 3:** Agreement for Using a School Device at Home.
 - **Appendix 4:** Parent/Guardian Agreement.
-

Appendix 1: Online Safety Rules for Pupils

As part of online safety lessons, each class will design and present their online safety rules, using these guidelines to ensure safety and responsible behaviour online.

I want to stay safe while using technology, so I will:

- **Only use the internet when an adult says it's OK.**
 - **Keep my personal information private** (name, address, phone number, and passwords).
 - **Only visit websites that my teacher or an adult has agreed on.**
 - **Tell an adult if I see something that upsets me or makes me feel uncomfortable.**
 - **Be respectful and kind when I am online or sending messages.**
 - **Never agree to meet someone I've met online in person without my parent or carer's permission.**
 - **Not send inappropriate or mean messages.**
 - **Keep my password safe and never share it with anyone.**
 - **Never take photos of others without permission or share them without consent.**
 - **Not download or install anything without permission.**
 - **Always ask an adult if I need help online.**
-

Appendix 2: Acceptable Use Agreement for Staff, Governors, Volunteers, and Visitors

By using The Eden School's IT systems and accessing the internet within the school, or outside the school on a school-provided device, I agree to the following rules:

- **I will not access inappropriate material**, including violent, criminal, or pornographic content.
- **I will use the school's systems for educational purposes only** and not for personal use during work hours.
- **I will not install any unauthorised software** or connect unauthorised hardware to the school's network.
- **I will not share my password** with others and will keep my login details secure.
- **I will not share confidential information** regarding the school, its pupils, or staff with unauthorised persons.
- **I will follow the school's data protection and safeguarding policies** to ensure the protection of sensitive data.
- **I will report any suspicious or inappropriate activity** to the Designated Safeguarding Lead (DSL) or ICT Manager immediately.
- **I will take steps to protect all school devices**, keeping them secure and password-protected when used outside school.
- **I understand that the school may monitor my use** of its IT systems and internet access.

By signing below, I confirm I have read and understand this agreement.

Name: _____

Signature: _____

Date: _____

Appendix 3: Agreement for Using a School Device at Home

I understand that:

- The school device loaned to me is for **educational purposes** only and must not be used for significant personal use.
- I will take care of the device and ensure it is used responsibly.
- **I will not install any unauthorised software** on the device.
- I will use only school-approved accounts and services when using the device.
- Any sensitive data, including photos or videos of pupils, must be used for educational purposes and deleted after use.
- I will immediately report to the school if the device is lost, damaged, or stolen, and follow all steps to safeguard data.
- If I leave the school, I will return the device before my final day of work or schooling.
- The school may request the device at any time for maintenance, inspection, or retrieval.

Name of Pupil/Staff: _____

Signed: _____

Date: _____

Appendix 4: Parent/Guardian Agreement

The Eden School has agreed to loan a Chromebook or other digital device to your child for educational purposes. By signing this agreement, you agree to the following terms and conditions:

- The device is the property of **The Eden School** and should be used solely for educational purposes.
- **I will ensure my child uses the device responsibly**, including avoiding food and drinks near the device.
- The school may monitor the device remotely and **check for compliance with the school's acceptable use policies**.
- Any damage or loss must be reported immediately, and I will ensure the device is not used for unauthorised activities.
- The school retains the right to request the return of the device at any time for inspection or in the case of withdrawal from the school.
- **I understand the importance of online safety** and will monitor my child's use of the device at home to ensure it is used appropriately.

Pupil's Name: _____

Parent/Guardian Name: _____

Signed (Parent/Guardian): _____

Date: _____