Aspiration & Achievement | Resilience & Responsibility | Courage & Confidence

47 Online Safety Policy

Adopted May 2026

Review May 2027

See EOTAS policy control document (held by the Business Manager) for status, notes and actions about this policy

Contents

The implementation of this Online Safety policy will be monitored by the:	**Designated Safeguarding Lead, GDPR Compliance Officer / Business Support Manager**
The Management Committee will receive a report on the implementation of the Online Safety Policy generated by the Designated Safeguarding Lead/Deputy Designated Safeguarding Lead Team (which will include anonymous details of online safety incidents) at regular intervals:	**Annually**
The Online Safety Policy will be reviewed annually or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	**September 2026**
Should serious online safety incidents take place, the following external persons/agencies should be informed:	**LA Safeguarding Officer, LADO, Police**

This Online Safety Policy outlines EOTAS' commitment to creating a safe, inclusive, and accessible digital environment for all pupils regardless of their needs. It defines legal responsibilities, key areas of online risk, roles of stakeholders, incident reporting procedures, and strategies for fostering digital resilience. The policy aligns with key legislation such as the Online Safety Act (2023), Equality Act (2010), and UK GDPR, ensuring legal compliance and safeguarding best practices.

1. Purpose

At EOTAS, we recognize the transformative power of the digital world in enhancing education, communication, and personal development. However, we also acknowledge the potential risks associated with online environments. Our goal is to create an inclusive, accessible, and safe digital environment that caters to the diverse abilities of our school community.

Our objectives are to:

- Develop robust protocols that secure online spaces while ensuring accessibility for all students.
- Identify vulnerable groups who may face elevated online risks and provide tailored support strategies.
- Foster a culture of responsible, informed, and inclusive technology use through targeted education and awareness campaigns.
- Implement responsive systems for detecting, addressing, and escalating online safety incidents with consideration for students' diverse needs. This policy applies to everyone connected to the school community, whether accessing ICT resources on-

site or remotely.

2. Legal Framework and Guidelines

Legislation/Guidance	Purpose	Relevance to Online Safety
Keeping Children Safe in Education (KCSIE)	Safeguarding statutory guidance from the DfE	Provides protocols for online safety and safeguarding in schools
The Equality Act (2010)	Anti-discrimination legislation	Ensures equal access to digital resources for all students
Online Safety Act (2023)	New online safety framework	Mandates effective monitoring and reporting of online risks
Data Protection Act (2018) & UK GDPR	Regulates data protection and privacy	Protects student data, outlining secure handling of information
Special Educational Needs	Provides guidance for supporting students with SEND	Emphasizes inclusive practices in online safety
Public Sector Bodies Accessibility Regulations (2018)	Accessibility standards for digital platforms	Ensures all online content meets accessibility requirements

This policy aligns with statutory guidelines and legislation, ensuring a robust approach to online safety and digital inclusion at EOTAS. The key legal frameworks that underpin this policy include:

• **Keeping Children Safe in Education (KCSIE) (DfE):** Provides statutory guidance on safeguarding children, including online safety protocols for schools.

• **The Education Act (1996, 2006, 2011):** Outlines the duties of schools to promote the welfare of children, including responsibilities related to digital safeguarding.

• **The Equality Act (2010):** Mandates equal access to education and digital resources for all students, ensuring non-discrimination based on disability, gender, race, religion, or other protected characteristics.

• **Online Safety Act (2023):** Establishes clear responsibilities for educational institutions to safeguard students from online harms, including cyberbullying, harmful content, and online exploitation. The Act also requires schools to implement effective monitoring, f iltering, and reporting mechanisms.

• **The Data Protection Act (2018) and UK GDPR:** Regulate the collection, storage, and processing of personal data, emphasizing the protection of students' digital information.

• **Freedom of Information Act (FOIA):** Ensures transparency in the handling of public information, including digital records maintained by schools.

• **Special Educational Needs and Disability (SEND) Code of Practice:** Provides statutory guidance on the duties of schools to support students with SEND, including digital accessibility and online safety considerations.

• **Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations (2018):** Requires public sector organizations, including schools, to meet accessibility standards for digital content, aligning with WCAG 2.1 guidelines.

EOTAS' online safety protocols are regularly reviewed to ensure compliance with these legal requirements, fostering a safe, inclusive, and legally compliant digital environment.

Key Areas of Online Risk

Risk Category	Definition	Support Strategies
Content	Exposure to harmful or inappropriate material	Filtering systems, staff monitoring, student education on critical thinking
Contact	Risks from online interactions like cyberbullying or grooming	Clear reporting mechanisms, social skills training, digital resilience programs
Conduct	Unsafe online behaviors like oversharing personal data	Digital citizenship lessons, peer mentoring, behavior policies
Commerce	Financial risks from scams or online fraud	Educating students on identifying scams, safe online purchasing practices

Our online safety strategy focuses on four main risk categories:

• **Content:** Involves exposure to inappropriate, harmful, or misleading digital material, including content that could cause distress due to violent, explicit, or discriminatory themes.

• **Contact:** Encompasses the risks posed by interactions with others online. This includes threats such as cyberbullying, grooming, manipulation, and online exploitation. We recognize that some students may face additional challenges in recognizing when interactions are unsafe, and we are committed to providing clear, accessible guidance to help them identify, report, and manage such risks.

• **Conduct:** Refers to the ways students behave online, including the risks associated with sharing personal information, engaging in inappropriate behavior, or participating in unsafe digital activities. For students with SEN, we deliver personalized digital citizenship education, promoting understanding of respectful communication, privacy, and digital boundaries.

• **Commerce:** Relates to the financial risks that arise from online activities, including exposure to scams, fraudulent schemes, and misleading advertising. We provide targeted

support to help students with cognitive disabilities understand the potential dangers of online transactions and develop critical thinking skills to navigate these situations safely.

3. **Curriculum and Awareness Measures**: EOTAS integrates online safety into the curriculum to ensure that all students, regardless of ability, receive age-appropriate and accessible education about the digital world. We provide tailored resources and teaching strategies to meet the diverse learning needs of our students, including those with special educational needs (SEND).

Key Focus Areas:

• **Digital Literacy:** Empowering students to use technology effectively and responsibly.

• **Online Behavior:** Teaching respectful communication, digital etiquette, and the consequences of cyberbullying.

• **Data Privacy:** Educating students on the importance of protecting personal information.

• **Critical Thinking:** Encouraging students to question the reliability of online content and recognize misinformation.

• **Accessibility in Learning:** Utilizing assistive technologies and differentiated instruction methods to support all learners. Our curriculum is regularly reviewed to ensure it reflects current risks and technological developments, with a focus on fostering digital resilience in every student.

Definitions for Filtering and Monitoring

• Filtering: Technology that blocks harmful content while considering the specific needs of students, such as avoiding over-blocking that may hinder accessibility tools.

• Monitoring: Systems designed to detect risky online activities with adaptive alerts tailored to students' varying communication styles and behaviors.

Standards for Compliance.

• Clear roles and responsibilities for digital safety oversight, with SEN considerations embedded.

• Regular reviews of filtering and monitoring systems to ensure they support both safety and accessibility.

• Inclusive content management practices that do not unintentionally restrict access to beneficial assistive technologies.

• Flexible monitoring strategies to accommodate different learning needs and abilities.

• Compliance with the **Online Safety Act (2023)** to ensure risks such as cyberbullying, online harassment, and harmful content are actively identified and mitigated within the school's digital environment.

• Full adherence to the **Equality Act (2010),** ensuring that online safety practices promote equal opportunities, address discrimination, and support accessibility for all students, especially those with disabilities.

Implementation of the **Accessibility Standards for Schools**, ensuring that all digital platforms meet the accessibility requirements set by the Public Sector Bodies Accessibility Regulations 2018 and WCAG 2.1 standards.

4. Responsibilities

Role	Key Responsibilities	Focus Area
Governing Body	Oversight of online safety policies, regular reviews, assigning responsibilities	Ensuring legal compliance
DSL	Implementation of inclusive digital safety strategies, Managing incidents, leading online safety training	Staff training, safeguarding culture, Incident response, reporting
Romero	Ensuring secure and accessible technology	Monitoring systems, assistive tech
All Staff	Promoting responsible online behavior, recognizing risks	Classroom management, role modeling
Parents/Carers	Supporting online safety at home	Digital awareness Collabaration

Management Committee

• Ensure online safety is integrated into the broader safeguarding strategy, with a focus on inclusivity.
• Assign an Online Safety Management Committee Member: Gemma Meiklejohn responsible for overseeing online safety, accessibility, and SEN considerations.
This member of the management committee will:
o Monitor the implementation and effectiveness of online safety policies. o Ensure regular audits of digital safeguarding practices are conducted.
o Liaise with the Designated Safeguarding Lead (DSL) to review incident reports and online safety training.
o Advocate for continuous improvements in online safety, particularly in relation to accessibility and compliance with legal requirements.
• Regularly review the effectiveness of digital safety protocols, especially their impact on students with disabilities.
• Oversee the school's compliance with the Online Safety Act (2023), ensuring robust mechanisms are in place for reporting and addressing online harms.
• Ensure all digital safety practices align with the principles of the Equality Act (2010) and the Accessibility Standards for Schools, promoting fairness and equal access to online resources.
• Ensure online safety is integrated into the broader safeguarding strategy, with a

focus on inclusivity.
• Assign a member of the management committee responsible for monitoring online safety, accessibility, and SEN considerations.
• Regularly review the effectiveness of digital safety protocols, especially their impact on students with disabilities.
• Oversee the school's compliance with the Online Safety Act (2023), ensuring robust mechanisms are in place for reporting and addressing online harms.
• Ensure all digital safety practices align with the principles of the Equality Act (2010) and the Accessibility Standards for Schools, promoting fairness and equal access to online resources.

Headteacher
• Oversee the development of inclusive online safety practices.
• Promote a culture where digital accessibility and safety are seen as interconnected
• Implement measures outlined in the Online Safety Act (2023) to manage online risks within the school.
• Uphold the principles of the **Equality Act (2010)** and the **Accessibility Standards for Schools** in all digital safeguarding practices, fostering an environment of respect and inclusion.

Designated Safeguarding Lead (DSL)

• Act as the lead on online safety, with specialized knowledge of accessibility issues.
• Coordinate responses to incidents & provide regular reports on online safety.
• Ensure that all online safety concerns are documented and responded to in compliance with the **Online Safety Act (2023).** Promote the values of the and ensure digital platforms comply with the Accessibility Standards for Schools.

Romero

• Implement technology solutions that balance safety with accessibility.
• Conduct regular audits to identify potential barriers in digital platforms, ensuring compliance with WCAG 2.1.
• Support assistive technology integration while maintaining robust security measures.
• Apply the technical standards required under the **Online Safety Act (2023)** to enhance digital protections. • Ensure digital systems are compliant with the **Equality Act (2010) and the Accessibility Standards for Schools,** providing accessible learning tools for all students.

All Staff
• Embed online safety and accessibility into daily teaching practices.
• Participate in training on inclusive digital practices, online safety, and digital accessibility standards.
• Understand their role in upholding the principles of the **Online Safety Act (2023)** within the educational environment.
• Foster an inclusive digital environment that aligns with the **Equality Act (2010)** and

the **Accessibility Standards for Schools**, challenging any discriminatory behavior online.

Parents/Carers

• Support safe and inclusive technology use at home.
• Engage in school workshops that focus on online safety and digital accessibility.
• Collaborate with the school to identify and address specific online risks for their children.
• Be informed about the **Online Safety Act (2023)** and its implications for children's online safety.
• Understand the school's commitment to the **Equality Act (2010)** and the **Accessibility Standards for Schools**, supporting their child's digital rights and access.

5. Incident Reporting and Response Procedures

EOTAS has a clear process for reporting, investigating, and responding to online safety incidents to ensure timely intervention and support.

Reporting Process:

- **Step 1**: Any member of the school community (students, staff, parents) can report an incident to the Designated Safeguarding Lead (DSL) or a trusted staff member.
- **Step 2:** The DSL or trusted staff member logs the incident on CPOMS.
- **Step 3:** The incident is investigated by the DSL, in collaboration with relevant staff, such as the Romero if technical analysis is required.
- • **Step 4:** Appropriate action is taken, which may include support for the affected individuals, disciplinary measures, and, if necessary, referral to external agencies (e.g., police, child protection services). • Step 5: A review of the incident to identify lessons learned and improve policies or procedures if needed.

6. Staff Training and Development All staff receive ongoing training to stay updated on online safety risks and best practices, with a focus on supporting students with SEND. Training Includes:
• Annual safeguarding and online safety training.
• Training on the use of assistive technologies, including AI and inclusive digital teaching practice

7. Risk Assessment Framework EOTAS conducts regular risk assessments to evaluate potential threats related to online activities, especially when introducing new technologies.

Key Aspects:

• Identifying risks related to new software, apps, or devices.
• Assessing the impact of online activities on students with specific needs.

- Developing mitigation strategies for identified risks.

8. Partnerships with External Agencies

EOTAS collaborates with local and national organizations to strengthen online safety efforts:

- CEOP (Child Exploitation and Online Protection Command): For reporting online abuse.
- Swindon Safeguarding Partnership: For policy guidance and incident escalation

9. Monitoring and Evaluation

The effectiveness of this policy is evaluated annually through:

- Analysis of incident reports.
- Feedback from staff, students, and parents.
- Regular audits of digital systems and online safety practices.

10. Glossary of Key Terms

- **CEOP:** Child Exploitation and Online Protection Command.
- **Cyberbullying:** Bullying that takes place over digital devices.
- **Filtering: Technology** that restricts access to harmful online content.
- **Monitoring:** Tools used to detect and respond to online safety risks.
- **SEN:** Special Educational Needs.
- **DSL:** Designated Safeguarding Lead.

11. Alignment with Safeguarding Policies

This Online Safety Policy aligns with key safeguarding documents to provide a holistic approach to student welfare, including:

- **Safeguarding & Child Protection Policy:** Ensures online risks are addressed within broader safeguarding frameworks.
- **Anti-Bullying Policy:** Tackles cyberbullying with consistent approaches across online and offline environments.
- **Behaviour Policy:** Defines expectations for digital conduct alongside general behavior standards.

12. Digital Wellbeing

EOTAS promotes healthy digital habits to support student wellbeing.

We focus on:

• **Screen Time Management:** Encouraging balanced use of technology.

• **Digital Detox:** Promoting offline activities to support mental health.

• **Mindful Technology Use:** Teaching students to reflect on how technology impacts their mood and behavior.

13. Policy Breaches and Consequences

Clear consequences are outlined for breaches of the Online Safety Policy:

• **For Students**: Restorative conversations, parental involvement, and possible disciplinary measures.

• **For Staff:** Investigations under the Staff Code of Conduct with appropriate disciplinary actions if necessary.

• **For Parents/Carers:** Restricted access to school systems where relevant, with guidance provided on appropriate digital behaviors.

14. Emerging Technologies

EOTAS continuously assesses risks from new technologies, such as:

• AI and Deepfake Content: Educating students on how to identify manipulated digital media.

• Virtual Reality (VR) and Augmented Reality (AR): Ensuring safe use of immersive technologies.

• Educational Technology (EdTech): Regularly reviewing EdTech tools to ensure they are secure, accessible, and support inclusive learning.

This includes

o Assessing the privacy and data security of EdTech applications.

o Evaluating the accessibility features of tools to support students with disabilities.

o Providing staff with training to effectively integrate EdTech in a way that enhances learning while maintaining online safety.

15. Data Protection & Privacy Awareness

We ensure all members of the school community understand:

• How personal data is collected, stored, and used.

• Students' rights under the Data Protection Act (2018) and UK GDPR.

• Safe data-sharing practices, especially on social media and public platforms.

16. Annual Policy Review Process

The Online Safety Policy is reviewed annually through:

• Stakeholder Feedback: Involving staff, students, parents, and governors.

• Policy Audits: Reviewing incidents and emerging risks to inform updates.

• Governance Oversight: The Safeguarding management committee member leads the review process, ensuring compliance with legal and regulatory standards.

17. Accessibility Statement

EOTAS is committed to making this Online Safety Policy accessible to everyone, including individuals with visual, auditory, cognitive, and motor impairments. The policy is available in alternative formats upon request, and efforts are made to ensure:

- **Clear, plain language is used throughout.**
- **Documents are compatible with screen readers and assistive technologies.**
- **Availability in Accessible Formats:** The policy is provided in formats such as large print and audio versions upon request to support students, staff, and parents with specific accessibility needs.
- **Easy-Read Versions:** Simplified, easy-to-read versions with visual aids are available to make key information more accessible to individuals with learning difficulties. Our commitment extends beyond compliance, ensuring that every member of our school community can understand and engage with the content of this policy effectively.

18. Child-Friendly Version of the Policy

EOTAS is committed to making online safety accessible to all pupils, including those with additional learning needs. A child-friendly version of this policy can be provided with simplified language, visuals, and key online safety rules to help students understand how to stay safe online.

19. ICT Acceptable Use Policy To promote responsible technology use

EOTAS has an ICT Acceptable Use Policy for both staff and students, outlining expectations for: • Respectful use of devices and online platforms. • Protecting personal information and data. • Following online etiquette and digital citizenship principles. • Reporting inappropriate content or behavior.

20. Remote Learning Safeguarding Protocols

In remote or hybrid learning environments, safeguarding remains a top priority. The following Remote Learning Safeguarding Protocols apply:

• Clear expectations for online classroom behavior.

• Secure login procedures to protect student privacy.

• Guidelines for safe video conferencing, including background settings and camera use.

• Recording lessons only with appropriate permissions for safeguarding purposes.

21. Collaboration with Law Enforcement

EOTAS works closely with law enforcement agencies to address serious online safety concerns. In cases involving illegal activities, such as grooming, online exploitation, or cybercrime:

• The Designated Safeguarding Lead (DSL) will report incidents to the appropriate authorities.

• Evidence related to online offenses will be preserved following legal protocols.

• The school will cooperate fully with police investigations while maintaining student confidentiality where appropriate.

22. Evaluation and Continuous Improvement Plan

To ensure continuous improvement, Crowdys Hill School evaluates the effectiveness of this policy annually by:

• Conducting staff, student, and parent surveys on online safety awareness.

• Reviewing online incident reports to identify trends and areas for development.

• Gathering feedback through focus groups and school council discussions.

• Adjusting policy content based on new risks, technological changes, and stakeholder feedback.

Frequently Asked Questions (FAQs)

1. **What should I do if my child experiences cyberbullying?**
   o Encourage them to speak to a trusted adult, report it to the DSL, and avoid responding to the bully.
2. **How does the school monitor online activity?**
   o We use filtering and monitoring tools to detect harmful content while respecting privacy and accessibility needs.
3. **Can students bring personal devices to school?**
   o Personal device policies vary; please refer to the ICT Acceptable Use Policy section.

23. Data Breach Response Plan

In accordance with the **Data Protection Act (2018)** and **UK GDPR,** the school has a clear Data Breach Response Plan:

• Identification: All staff must report suspected data breaches immediately to the Data Protection Officer (DPO) – Evan James or DSL – Sally Banks.

• Containment: Immediate steps are taken to contain the breach and minimize data exposure.

• Investigation: A full investigation determines the cause, extent, and impact of the breach.
• Notification: If necessary, affected individuals and the Information Commissioner's Office (ICO) will be notified within the legal timeframe (72 hours).

• Review: Lessons learned from breaches inform future data protection practices.

24. Staff Personal Use of Social Media Guidelines

Staff are expected to maintain professional boundaries online. The following Social Media Guidelines apply:

- Staff should avoid accepting or sending friend requests to current students.
- Personal social media accounts must not be used to communicate with students or parents.
- Any concerns about online interactions involving students must be reported to the DSL.
- Staff must not share confidential school information on personal social media platforms.

Quick Reference Guide

• Report Concerns To: Designated Safeguarding Lead (DSL) or any trusted staff member.

- Key Contacts:
  - o DSL: sally.banks@eotas.swindon.sch.uk
  - o Management Committee Member with Online Safety oversight: Gemma Meiklejohn

- **Key Steps to Report an Online Safety Issue:**

1. Recognize the issue.
2. Report it immediately to the DSL.
3. Support investigations if required.
4. Follow up to ensure appropriate action was taken.

- **Top 3 Online Safety Tips:**

1. Never share personal information online.
2. Report any inappropriate or uncomfortable online behavior.
3. Think critically about the content you see and share.

References

This policy has been informed by key resources and statutory guidance, including:

- NSPCC Learning: The 4 Cs of online safety | NSPCC Learning
- Keeping children safe in education - GOV.UK
- Online Safety Act 2023
- Equality Act 2010
- Data Protection Act 2018
- Freedom of Information Act 2000

Appendices

This policy has been informed by key resources and statutory guidance, including

- NSPCC Learning: The 4 Cs of online safety | NSPCC Learning
- Keeping children safe in education - GOV.UK
- Online Safety Act 2023
- Equality Act 2010
- Data Protection Act 2018
- Freedom of Information Act 2000

Privacy notice for parents/carers – use of your child's personal data

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. This privacy notice explains how we collect, store and use personal data about pupils. We, EOTAS, are the 'data controller' for the purposes of data protection law. Our data protection officer is Evan James (see 'Contact us' below).

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department