



Online Safety Policy

FOREST OF DEAN TRUST

Policy name	Online Safety Policy
Version date	June 2026
Owner	SBo
Approval date	23rd June 2026
Approver	Trustees
Review frequency	Annually
Review date	June 2027

1. Introduction

The Trust recognises the importance of online safety in protecting students, staff, and stakeholders across all settings. This policy aims to ensure that technology is used responsibly, securely, and safely, promoting a culture of digital resilience and safeguarding within the Trust.

2. Purpose of the Policy

The policy is designed to:

- Protect students and staff from risks associated with digital technologies.
- Promote safe and responsible use of the internet and digital devices.
- Establish clear guidelines for the appropriate use of online resources.

3. Scope

This policy applies to:

- All students, staff, members, governors, trustees, and volunteers within the Trust.
- Use of technology both on and off Trust premises, including school networks, personal devices, and online platforms.
- All forms of digital communication, including email, social media, websites, and learning platforms.

4. Roles and Responsibilities

- **Trust Leadership Team:** Oversee online safety policies and ensure compliance with relevant legislation. Trustees hold ultimate responsibility for ensuring that filtering and monitoring systems are robust.
- **Designated Safeguarding Lead (DSL):** Monitor and address online safety concerns, providing training and support while also defining the level of internal access suitable across the trust.
- **Pastoral Team :** Will support the DSL to aid with the monitoring and addressing of concerns around digital and online safety.
- **ICT Staff:** Implementing and maintaining filtering and safeguarding technology to support the DSL advice.
- **DPO :** School Pro are currently contracted as the trusts DPO. They will work with the schools to improve data protection, and online safety within all schools.
- **Staff:** Implement this policy and model appropriate online behaviour.
- **Students:** Use digital technologies responsibly, following guidance provided by the Trust.
- **Parents/Carers:** Support the Trust's online safety measures and reinforce responsible digital behaviours at home.

5. Guidelines for Staff

- **Professional Use:**
 - Use school-provided devices and accounts for all professional communications, following communication guidelines.
 - Maintain professional boundaries with students on all digital platforms as set out in the social media policy.
- **Safeguarding:**
 - Report any online safety concerns, including inappropriate content or cyberbullying,

to the DSL immediately.

- Do not share personal information or engage in private conversations with students via personal accounts.

- **Data Security:**

- Follow GDPR guidelines when handling student data as detailed in the trusts Data Protection Policy.
- Ensure strong passwords and secure storage of devices.

- **Social Media:**

- Refer to the Trust's Social Media Policy for appropriate online engagement.

- **Artificial Intelligence**

- only use trust recommended AI tools
- protect data privacy (never input student names, or personal data into public AI tools)

6. Guidelines for Students

- **Safe Internet Use:**

- Only access age-appropriate content on school devices and networks.
- Never share personal information online, including passwords, addresses, or phone numbers.

- **Respectful Behavior:**

- Use technology respectfully and responsibly, avoiding cyberbullying or sharing harmful content.
- Report any online issues to a trusted adult, teacher, or the DSL.

- **Personal Devices:**

- *Primary Education* – personal devices (such as smartphones and smartwatches) are strictly prohibited during the school day.
- *Secondary education* – Personal devices must remain off and out of sight or put in secure lockers during school hours, unless explicitly permitted by a member of staff.
- Do not attempt to bypass school internet security systems.

- **Artificial Intelligence**

- AI tools are a useful learning tool, but should be used ethically to support learning and not as a plagiarism tool.
- There are risks associated with AI tools students should be aware of deepfakes and AI generated misinformation.

7. Monitoring and Filtering

- **School Networks:**

- The Trust will use robust filtering and monitoring systems to block harmful or inappropriate content. These systems monitor the Content, Contact, Conduct and Commerce (as per the Keeping Children Safe in education guidelines)
- Regular audits of network activity will ensure compliance with this policy.
- Alerting will be provided to the DSL to give assurance

- **Student Activity:**

- Staff will monitor students' use of technology during lessons, using in-class monitoring tools such as Senso and Imperio, and report concerns.

8. Online Learning and Remote Education

- **Secure Platforms:**
 - Only approved platforms should be used for online learning and communication.
 - Virtual sessions must follow safeguarding guidelines, including the presence of multiple staff where necessary.
- **Staff Conduct:**
 - Maintain the same professional standards as in physical classrooms during online interactions.
- **Student Expectations:**
 - Follow the Trust's behaviour and online safety rules during remote learning.

9. Responding to Online Safety Concerns

- **Reporting:**
 - All online safety incidents must be reported to the DSL.
 - The Trust's safeguarding policy outlines procedures for handling concerns, including liaison with external agencies.
- **Cyberbullying:**
 - Incidents will be addressed under the Trust's anti-bullying policy.

10. Training and Awareness

- **Staff:**
 - All staff will receive regular online safety training, including recognising risks and safeguarding protocols.
 - DSL and ICT team members will be offered additional training around best practise and the tools used to enforce/monitor this.
- **Students:**
 - Online safety will be integrated into the curriculum to develop digital literacy and resilience.

11. Review and Updates

This policy will be reviewed annually or in response to significant technological or legislative changes.

Version Control

Version	Summary of changes	Author	Date
1.0	Creation	Stephen Bourne	June 2026
1.1	Added AI references, clarification around monitoring and filtering (KCSIE) and linking to the DPO	Stephen Bourne	June 2026