

Online Safety Policy

Drafted By	Governance Lead
Review By	Network Manager
Status & Review Cycle	Annual
Next Review Date	Spring 2027

1. Introduction

Tandridge Learning Trust is committed to ensuring that all pupils, staff, trustees, governors, and visitors are safe online. This policy outlines our approach to online safety across the Trust. It supports our statutory safeguarding duties and aligns with Keeping Children Safe in Education (KCSIE), the Department for Education (DfE) filtering and monitoring standards, the UK GDPR, Data Protection Act 2018, the Artificial Intelligence Policy and other relevant guidance.

2. Aims

The aims of this policy are to ensure that:

- All members of the Trust community are protected from online harm.
- Staff understand their responsibilities in safeguarding pupils online.
- Pupils develop digital literacy skills and behave responsibly online.
- Systems and technologies across the Trust are secure and appropriately monitored.
- Online safety incidents are managed consistently across the Trust.

3. Scope

This policy applies to:

- All staff (including temporary, volunteers, supply, and contractors)
- All pupils
- All trustees, governors, and visitors
- All digital devices and platforms used within the Trust
- Any online activity linked to Trust systems or school life

4. Roles and Responsibilities

4.1 Trust Board:

- Ensure robust Trust-wide online safety arrangements
- Receive annual online safety reports
- Ensure compliance with safeguarding legislation
- Ensure appropriate filtering and monitoring systems are in place

4.2 Executive Board:

- Ensure consistent implementation across schools
- Provide strategic leadership, resources, and support

4.3 Local Governing Bodies (LGBs):

- Monitor school-level online safety practice
- Review online safety data and incident reports
- Ensure staff are trained in line with KCSIE guidance
- Ensure that pupils are taught how to keep themselves and others safe online

4.4 Designated Safeguarding Leads (DSLs) will

- Lead on online safety within their school including implementing this policy and ensuring appropriate systems and processes are in place
- Understand and regularly review the school's filtering and monitoring systems, working with the IT Network Manager and senior leaders.

Online Safety

- Ensure staff training is up-to-date
- Manage online safety concerns and referrals in line with KCSIE and school policy, including cyber bullying
- Liaise with external agencies where required
- Undertaking annual risk assessments

4.5 IT Network Manager will

- Ensure the security procedures are appropriate so that pupils are kept safe
- Ensure systems are secure and protected against viruses and malware
- Maintain secure filtering and monitoring systems.
- Ensure device and system security (updates, patching, access control).
- Report online safety concerns to DSLs.

4.6 All Staff and volunteers will

- Follow this policy and the Staff Acceptable Use Agreement
- Report online safety concerns promptly
- Model safe online behaviour
- Teach or support the delivery of online safety education
- Ensure any cyber bullying is dealt with in line with the behaviour policy

4.7 Parents/Carers are expected to

- Support safe use of devices at home
- Raise any concerns with a member of staff or headteacher
- Work collaboratively with the Trust on online safety matters.

5. Education and Curriculum

5.1 Pupils

The curriculum will include:

- Digital literacy
- Safe use of social media
- Managing online relationships
- Cyberbullying awareness
- Online reputation
- Privacy, data, and healthy online habits
- Recognising online risks (e.g., grooming, radicalisation, scams)
- Recognising and responding to online sexual exploitation and coercion (including sextortion).
- Understanding misinformation and AI-generated content (including deepfakes) and how to report concerns.

Online safety will be taught through:

- Computing curriculum
- PSHE/RSE curriculum
- Assemblies
- Theme days / workshops

5.2 Staff

Staff will receive regular online safety training including:

Online Safety

- Reporting procedures
- Online safeguarding risks
- Appropriate use of technology
- Use of Trust systems and data security

6. Technology, Filtering & Monitoring

The Trust will implement:

- Age-appropriate filtering aligned with legal requirements
- Continuous or regular monitoring of online activity
- Secure user authentication and password policies
- Encrypted devices and secure networks
- Remote access controls

The Trust uses filtering and monitoring that meets **DfE standards for filtering and monitoring**.

Monitoring may include (where proportionate) review of internet use, search activity, emails/messages, files and device activity on Trust systems. Monitoring is for safeguarding, security and policy compliance. Users should have no expectation of privacy when using Trust systems, except where required by law, and monitoring will be carried out fairly and transparently in line with data protection requirements.

7. Acceptable Use

Acceptable Use Agreements (AUAs) will be in place for:

- Staff
- Pupils (age-appropriate versions)
- Governors/trustees
- Visitors where relevant
- Non-compliance may result in action in line with relevant Trust policies (for example, disciplinary, conduct or behaviour policies).

8. Responding to Incidents

Any online safety incident will be:

1. Reported to the DSL (or Deputy DSL).
2. Recorded using the Trust's safeguarding system.
3. Investigated and managed using safeguarding procedures.

Incidents may include:

- Cyberbullying
- Online sexual harassment
- Online grooming, exploitation or coercion (including sextortion).
- Sharing of sexual images (including 'sexting' and AI-generated sexual images).
- Exposure to harmful content
- Illegal content
- Data breaches
- Technology misuse

Online Safety

The Trust follows appropriate referral pathways including police, LADO, and children's social care. Where an incident involves a data protection breach, the Trust will follow its Data Breach policy. Incidents linked to extremism will be managed in line with the Prevent Duty.

9. Use of Digital and Social Media Platforms

The Trust will:

- Use official social media accounts only
- Ensure content is appropriate, secure and compliant
- Not share pupils' personal information without consent
- Provide guidance to staff on their personal social media use

10. Remote Learning

Where remote learning is used, the Trust will:

- Use approved platforms only
- Ensure safeguarding measures are in place
- Provide guidance to parents
- Ensure staff follow professional expectations

11. Monitoring, Reporting and Review

- The DSL in each school will maintain online safety logs.
- Trust-wide data will be reviewed termly.
- The Trust Board will receive an annual report.
- This policy will be reviewed annually or following significant updates in guidance or technology.