

		Date	Review Date
Written by	Debbie Goode	01/09/2026	01/09/2027
Reviewed by	Ryan Goodwin	01/09/2026	01/09/2027

Legal Status

This policy aligns with the Department for Education's statutory safeguarding guidance *Keeping Children Safe in Education (KCSIE 2026)* and its supporting advice on **Teaching Online Safety in Schools**, *Preventing and Tackling Bullying (including Cyberbullying)*, and the *Prevent Duty*.

It also reflects our statutory obligations under:

- Education Act 1996 (as amended)
- Education and Inspections Act 2006
- Education Act 2011
- Equality Act 2010
- Data Protection Act 2018
- **Online Safety Act 2023 (placing new duties on platforms to protect children from harmful content)**

Policy Applies to: -

- All staff (teaching and non-teaching) and volunteers working within TILT Education

Related Documents: -

- Keeping Children Safe in Education 2026
- E-Safety Acceptable Use Document
- Photography and image sharing guidance.
- Safeguarding Policy
- Behaviour for Success Policy
- Anti Bullying Policy
- PSHE & RSE Policy
- SEND Policy
- Spiritual, Moral, Social and Cultural Education Policy
- Statement of Equality

Availability

This Policy is made available to staff, parents and pupils, a paper copy may be obtained from TILT Education Office.

Monitoring and Review

This policy is subject to continuous monitoring, refinement, and audit by the Proprietors who are both the Head of Centre and Headteachers.

Policy Aims

At TILT Education, we hold that our pupils should never experience online abuse, whether within the school network or beyond. The internet provides valuable opportunities but also poses risks.

We believe:

- All children deserve safeguarding from online harm.
- Our duty extends to risks both inside and outside school.
- Safeguarding requires cooperation with pupils, parents, carers, and external agencies.
- Every child must have equal protection, regardless of background or protected characteristics.
- ICT systems must remain secure, filtered, and monitored.

Pupils may be exposed to risks including:

- Cyberbullying and online harassment
- Grooming, radicalisation, and extremist material
- Sexual abuse, exploitation, and sextortion
- Misinformation, disinformation, and conspiracy theories
- AI-generated deepfakes and harmful synthetic content

TILT Education understands that TILT Education must have strong ICT infrastructure and data protection practices; that TILT Education's ICT systems need to be managed in ways that ensure that TILT Education meets the DfE e-safety technical requirements.

TILT Education will be responsible for ensuring that the ICT infrastructure / network is as safe and secure as is reasonably possible and that ICT/ E-safety policies and procedures are implemented. To do this TILT Education will take appropriate security measures to protect wireless systems, work stations and hand held devices etc from accidental or malicious attempts which might threaten the security of TILT Education systems and data.

Roles and responsibilities

Proprietors (Head of Centre and Headteacher)

- Hold strategic accountability for safeguarding online.
- Ensure robust filtering, monitoring, and cyber resilience in line with DfE and NCSC standards.
- Receive regular safeguarding and ICT reports.

Designated Safeguarding Lead (DSL)

- Procures and oversees filtering and monitoring systems.
- Documents decisions on blocked/unblocked content.
- Reviews filtering and monitoring annually and after serious incidents.
- Coordinates responses to online concerns and escalates where necessary.

Staff

- Attend mandatory training on safeguarding and online safety.
- Comply with acceptable use expectations.
- Stay vigilant for online harms and record concerns promptly via LearnTrek (categories include cyberbullying, radicalisation, sexting, self-harm content).

The DSL with the support of the Headteacher will ensure that in in depth review of the filtering and monitoring system is completed at least annually.

To do this they will

- ensure filtering and monitoring meets the needs of our pupils and staff, and reflects the specific use of technology while minimising potential harms.
- evaluate the changing needs and potential risks.
- record for reference the results of the online review and make available to those entitled to inspect that information.

Filtering, Monitoring, and Technical Controls

We use filtering and monitoring systems that are:

- Age-appropriate and DfE-compliant.
- Effective in blocking harmful material such as:
 - Child sexual abuse material (CSAM)
 - Terrorist and extremist content
 - Gambling, ransomware, and illegal activity
 - Inappropriate pornography
 - Resilient against circumvention (e.g., VPN blocking, anonymising tools).

Technical details:

- Provider participates in IWF and CTIRU intelligence-sharing networks.
- Effectiveness tested annually using SWGfL tools.
- Logs capture device ID, time, and search terms.
- Systems reviewed against new threats such as generative AI abuse and disinformation.

Staff Training and Awareness

- All staff receive safeguarding and online safety induction training.
- Annual refresher training updates staff on emerging risks such as deepfakes, conspiracy theories, and AI misuse.
- DSLs undertake enhanced training to support colleagues effectively.

Educating Pupils and Parents

Pupils receive structured education in:

- Critical evaluation of online information.
- Recognising grooming and radicalisation.
- Safe use of social media and avoiding sexting.
- Identifying disinformation, conspiracy content, and AI-manipulated media.

Pupils are directed to trusted reporting tools such as CEOP.

Parents and carers are engaged through:

- Workshops and newsletters.
- Signposting to trusted online resources.
- Updates on Ofcom duties under the Online Safety Act 2023, including platform age verification and reporting requirements.

Managing Incidents

- All concerns are escalated immediately to the DSL.
- Responses may include internal interventions, sanctions, or external referrals (Police, social care, Prevent).
- Every incident is logged and reviewed to ensure lessons are learned.
- Post-incident, policies and technical systems are updated where necessary.

Review and Continuous Improvement

- Policy reviewed annually, or sooner if legislation changes.
- Filtering and monitoring systems reviewed **termly for effectiveness and annually in depth**.
- Proprietors receive safeguarding and ICT safety reports each term.

Appendix A – Technical Detail on Filtering and Monitoring

TILT Education recognises that effective technical controls are central to keeping children safe online. These details outline how our systems meet DfE and *Keeping Children Safe in Education 2026* requirements.

Filtering Systems

- Our filtering provider (BT) is:
 - A member of the Internet Watch Foundation (IWF).
 - Signed up to the Counter-Terrorism Internet Referral Unit (CTIRU).
 - Blocking access to illegal child sexual abuse material (CSAM) and unlawful terrorist content.
 - Filtering applies to all:
 - Internet feeds (including backup connections).
 - School-owned devices (on-site and off-site).
 - WiFi networks (encrypted and password-protected).
 - Filtering features include:
 - Age- and ability-appropriate restrictions.
 - Handling of multilingual web content, images, abbreviations, and misspellings.
 - Blocking circumvention methods such as VPNs and proxy services.
 - Real-time alerts when harmful content is blocked.
 - **Annual review** of filtering effectiveness includes:
 - Gaps in coverage and new risks (including AI-generated content).
 - Safeguarding reports and curriculum needs (e.g., PSHE).
 - Suitability for pupils with SEND or EAL.
 - Effectiveness is tested using the SWGfL filtering test tool (testfiltering.com).
-

2. Monitoring Systems

Monitoring complements filtering by tracking and alerting staff to user activity.

- Monitoring strategies include:
 - **Physical supervision:** Pupils are always supported by staff when online (minimum ratio 1 adult to 2 pupils).
 - **Network monitoring:** Log files of internet traffic and access are reviewed.
 - **Device monitoring:** Software installed on school devices generates alerts.
- Monitoring systems capture:

- Device ID, IP address, and (where possible) named user.
 - Time/date of access.
 - Search terms or content attempted.
 - Monitoring provision is reviewed at least annually, and after:
 - A safeguarding incident.
 - Introduction of new technology or practices (e.g., BYOD, remote access).
 - **Staff receive training** to interpret monitoring data and escalate safeguarding concerns effectively.
-

3. Reporting and Logging

- All safeguarding concerns linked to online safety are recorded in LearnTrek under the “E-Safety” category, with subcategories including:
 - Cyberbullying
 - Grooming / radicalisation
 - Child abuse images
 - Sexting or harmful sexual behaviour
 - Racist, sexist, homophobic, transphobic, or religious hate material
 - Terrorist or extremist content
 - Online gambling or illegal activity
 - Pornography (softcore/hardcore)
 - Hacking or bypassing security
 - **Other (staff specify details)**

Logs of checks include:

- Date and time of check.
 - Person responsible.
 - System/device checked.
 - Outcome and resulting actions.
-

4. Cybersecurity and Data Protection

- Servers, wireless systems, and cabling are securely located with restricted physical access.
 - Firewalls, antivirus, and intrusion detection systems are in place.
 - Data is managed in compliance with the Data Protection Act 2018 and UK GDPR.
 - All staff and pupils are assigned individual usernames and passwords.
 - Staff and pupils sign an **Acceptable Use Agreement** annually.
-

5. Limitations and Risk Mitigation

- No filtering or monitoring system is 100% effective.
- TILT Education mitigates this by:
 - Providing ongoing staff supervision.
 - Teaching digital resilience, critical thinking, and risk management.
 - Updating systems and policies in response to new threats.