		Date	Review Date
Written by	Debbie Goode	01/09/2025	01/09/2026
Reviewed by	Ryan Goodwin	01/09/2025	01/09/2026

Legal Status

This policy aligns with the statutory safeguarding guidance of the Department for Education, including Keeping Children Safe in Education (KCSIE 2025), 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

Policy Applies to

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

---

Related Documents

- Keeping Children Safe in Education 2025
- E-Safety Acceptable Use Document
- ICT SOW and Rational
- Drama and Communication SOW and Rational
- PSHE SOW and Rational
- Photography and Image Sharing Guidance
- Safeguarding Policy

- Positive Behaviour Policy
- Anti-Bullying Policy
- PSHE Policy
- SEND Non-Discrimination Policy
- SMSC Policy
- Statement of Equality

Availability

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

Monitoring and Review

This policy is subject to continuous monitoring, refinement, and audit by the Headteacher / Head of Centre.

Policy Aims

.

At TILT Education, we believe pupils should never experience online abuse, whether within the school environment or beyond. The internet provides valuable opportunities but also presents significant risks.

We believe:

- All children deserve safeguarding from online harm
- Safeguarding extends beyond the school environment
- Effective safeguarding requires partnership with pupils, parents, carers, and external agencies
- Every child must have equal protection regardless of background or protected characteristics
- ICT systems must be secure, filtered, and actively monitored

---

Online Risks

Pupils may be exposed to risks including:

- Cyberbullying and online harassment
- Grooming, radicalisation, and extremist content
- Sexual exploitation, sextortion, and abuse
- Misinformation, disinformation, and conspiracy theories
- AI-generated harmful or deceptive content (e.g., deepfakes)

ICT Infrastructure and Security

TILT Education ensures that ICT systems are safe, secure, and compliant with DfE expectations.

We:

- Implement robust security measures to protect systems and data
- Secure wireless networks, devices, and infrastructure
- Prevent unauthorised access and malicious attacks
- Maintain compliance with safeguarding and data protection requirements

---

Roles and Responsibilities

Proprietors (Head of Centre and Headteacher)

- Hold strategic accountability for online safeguarding
- Ensure effective filtering, monitoring, and cyber resilience
- Receive regular safeguarding and ICT reports

Designated Safeguarding Lead (DSL)

- Oversees filtering and monitoring systems
- Ensures systems are effective and appropriate
- Reviews systems annually and after serious incidents
- Coordinates safeguarding responses and escalations
- Maintains records of filtering and monitoring decisions

Staff

- Complete safeguarding and online safety training
- Follow acceptable use expectations
- Identify and report concerns via LearnTrek
- Remain vigilant to online risks

Monitoring and Review

The DSL, supported by the Headteacher, ensures that filtering and monitoring systems are reviewed annually and in response to incidents.

This includes:

- Evaluating effectiveness against pupil needs
- Identifying emerging risks

- Recording outcomes for inspection

Filtering, Monitoring, and Technical Controls

We use systems that are:

- Age-appropriate and compliant with DfE standards
- Effective in blocking harmful content
- Resilient to circumvention (VPNs, proxies)

Blocked content includes:

- Child sexual abuse material (CSAM)
- Terrorist and extremist content
- Pornography
- Illegal or harmful activity

Use of NetSweeper

We utilise NetSweeper as a key component of our safeguarding infrastructure. The system provides real-time, category-based filtering to prevent access to harmful and inappropriate content in line with Keeping Children Safe in Education and the Filtering and Monitoring Standards for Schools and Colleges.

In addition to filtering, NetSweeper provides active monitoring by logging and analysing user activity, including search terms, browsing behaviour, and attempts to access blocked content. The system applies intelligent categorisation and keyword recognition to identify patterns that may indicate safeguarding concerns, including exposure to harmful content, vulnerability indicators, or attempts to bypass controls.

Automated alerts are generated and directed to appropriate staff, including the DSL and IT leads. These alerts are reviewed promptly and form part of the school's safeguarding response procedures, including escalation through LearnTrek where required. This ensures that monitoring is proactive and enables early identification of risk, timely intervention, and effective safeguarding action.

Staff Training and Awareness

- All staff receive safeguarding and online safety training
- Annual updates include emerging risks (AI, disinformation, deepfakes)
- DSLs receive enhanced safeguarding training / CEOP training

---

Educating Pupils and Parents

Pupils are taught:

- How to recognise online risks
- Safe use of social media
- Critical thinking and identifying misinformation

- How to report concerns

Parents are supported through:

- Communication via our half termly newsletter, website and verbally
- Online safety guidance
- Updates on the Online Safety Act

Managing Incidents

- All concerns are reported to the DSL immediately
- Appropriate action is taken (internal or external)
- Incidents are logged and reviewed
- Systems and policies are updated following incidents

Review and Continuous Improvement

- Policy reviewed annually
- Systems reviewed termly and annually in depth
- Proprietors receive regular safeguarding reports

Appendix A – Technical Detail

1. Filtering Systems

- Provided via BT and NetSweeper
- IWF and CTIRU compliant
- Applies to all devices and networks
- Includes:
    - Age-appropriate filtering
    - Multilingual content handling
    - VPN and proxy blocking
    - Real-time alerts

---

2. Monitoring Systems

Monitoring is both technical and procedural.

We use NetSweeper to provide continuous monitoring of user activity. The system records web traffic, search activity, and attempts to access restricted content. It uses intelligent categorisation to identify potentially harmful behaviour and generates alerts based on safeguarding indicators such as self-harm, exploitation, extremism, or attempts to bypass controls.

Monitoring includes:

- Physical supervision of pupils
- Network and device monitoring
- Automated alert systems
- System checks including, keyword and SWGfl checks

Alerts are reviewed by trained staff, including the DSL, and form part of safeguarding procedures. Monitoring is active and supports early identification and intervention.

---

3. Reporting and Logging

All concerns are recorded in LearnTrek under E-Safety categories including:

- Cyberbullying
- Grooming / radicalisation
- Sexual content / sexting
- Extremism
- Hate content
- Pornography
- Security breaches

Logs include:

- Date/time
- Staff responsible
- Outcome/actions

---

4. Cybersecurity and Data Protection

- Secure infrastructure and restricted access
- Firewalls and antivirus systems
- GDPR compliance
- Individual user accounts
- Acceptable Use Agreements

---

5. Limitations and Risk Mitigation

No system is 100% effective.

We mitigate risk through:

- Staff supervision

- Pupil education
- Continuous system review
- Policy updates

Final Note

This policy ensures that TILT Education not only blocks harmful content, but also actively identifies, monitors, and responds to safeguarding risks.