

		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

1. Legal Framework and Statutory Guidance

This policy has been developed in accordance with the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education 2026, which came into force on 1 September 2026, and the DfE's Filtering and Monitoring Standards for Schools and Colleges.

The policy also takes account of the following legislation and guidance:

- Education Act 1996 (as amended)
- Education and Inspections Act 2006
- Education Act 2011
- Equality Act 2010
- Education Act 2002, where applicable
- Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)
- Online Safety Act 2023
- Prevent Duty guidance
- Teaching Online Safety in Schools
- Preventing and Tackling Bullying, including Cyberbullying
- DfE Digital and Technology Standards for Schools and Colleges
- National Cyber Security Centre (NCSC) guidance for schools

The Online Safety Act 2023 places duties on regulated online services. TILT Education recognises that these duties complement, but do not replace, the school's own safeguarding responsibilities.

Related Documents

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- E-Safety Acceptable Use Document
- Photography and Image Sharing Guidance
- Positive Behaviour Policy
- Anti-Bullying Policy
- Personal, Social, Health and Economic Education (PSHE) Policy

- SEND Non-Discrimination Policy
- Spiritual, Moral, Social and Cultural Education Policy
- Statement of Equality
- Data Protection and Privacy Notices
- Staff Code of Conduct

Availability

This policy is made available to staff, parents, carers and pupils. A paper copy may be obtained from the TILT Education office.

Aims and Principles

At TILT Education, we believe that all pupils have the right to access digital technology safely and to be protected from online harm, both within and beyond the school environment.

The internet provides valuable opportunities for learning, communication, creativity and personal development. However, it also presents risks that must be identified, managed and addressed through effective safeguarding arrangements.

TILT Education is committed to ensuring that:

- All pupils are protected from online abuse, exploitation and harmful content.
- Online safeguarding is an integral part of the school's wider safeguarding responsibilities.
- Appropriate filtering and monitoring systems are maintained across school technology.
- Staff understand their responsibilities for supervising pupils and reporting online concerns.
- Pupils receive age-appropriate and developmentally appropriate online safety education.
- Parents, carers and external agencies are involved in promoting online safety.
- Filtering and monitoring arrangements are regularly tested, evaluated and improved.
- Pupils with SEND receive appropriate support to understand online risks and develop safe digital behaviours.

TILT Education recognises that technical filtering and monitoring systems do not replace effective staff supervision, professional judgement or safeguarding procedures.

Our approach combines technical safeguards, direct supervision, education, reporting and regular review.

Understanding and Online Risks

TILT Education recognises that pupils may experience online risks both within school and through their use of technology outside the school environment.

Risks are considered within the four broad areas of online safety:

3.1 Content

Exposure to harmful or inappropriate material, including:

- Pornography and sexually explicit content.
- Material promoting self-harm, suicide or eating disorders.
- Terrorist, extremist or radicalising content.
- Racist, sexist, homophobic, transphobic or religious hate material.
- Violence, gambling and illegal activities.
- Misinformation, disinformation and conspiracy theories.
- AI-generated harmful content, including manipulated images and deepfakes.

3.2 Contact

Harmful interactions with others online, including:

- Grooming and sexual exploitation.
- Contact with individuals seeking to exploit or radicalise children.
- Online harassment, threats and intimidation.
- Manipulation, coercion and exploitation.

3.3 Conduct

Harmful behaviour involving online technology, including:

- Cyberbullying.
- Sharing inappropriate images or messages.
- Harmful sexual behaviour.
- Sextortion and image-based abuse.
- Misuse of social media.
- Attempts to bypass filtering or security controls.

3.4 Commerce

Risks associated with financial and commercial activity, including:

- Online gambling.
- Scams and fraudulent websites.
- Phishing and identity theft.
- Inappropriate advertising.
- Financial exploitation and pressure to make purchases.

Safeguarding pupils with SEND

TILT Education recognises that pupils with SEND may experience additional vulnerabilities when using digital technology.

Some pupils may have difficulties recognising unsafe situations, understanding online relationships, interpreting communication, identifying manipulation or reporting concerns.

Others may experience sensory sensitivities, communication difficulties, emotional regulation needs or challenges understanding the consequences of online actions.

TILT Education therefore ensures that online safeguarding arrangements reflect the individual needs of pupils.

This includes:

- Providing differentiated online safety education using accessible language, visuals, modelling and practical activities.
- Considering individual communication needs and ensuring pupils have accessible ways to report concerns.
- Providing direct staff support when pupils access online content.
- Adjusting filtering arrangements where appropriate to reflect age, developmental understanding and individual risk.
- Supporting pupils to recognise harmful or inappropriate online behaviour.
- Considering online vulnerabilities within individual risk assessments and support plans where relevant.
- Working with parents and carers to promote consistent online safety messages.

Filtering must protect pupils without unnecessarily restricting access to appropriate educational materials or opportunities to develop digital independence.

Any individual adjustments to filtering arrangements must be authorised, documented and reviewed

Roles and Responsibilities**5.1 Proprietors – Head of Centre and Headteacher**

The Proprietors retain overall strategic accountability for ensuring that TILT Education provides a safe digital environment.

They are responsible for:

- Ensuring appropriate filtering and monitoring arrangements are in place.
- Ensuring systems meet the school's safeguarding needs and are considered against DfE standards.
- Allocating sufficient resources for effective implementation and maintenance.
- Ensuring clear responsibilities are assigned for safeguarding and technical management.
- Receiving termly reports on filtering, monitoring, online incidents and identified risks.
- Ensuring an in-depth review is completed at least annually.
- Reviewing significant incidents, system weaknesses and required improvements.

- Ensuring appropriate staff training is provided.
- Overseeing cyber resilience and compliance with relevant data protection requirements.

5.2 Designated Safeguarding Lead (DSL) – Thomas Brookes

The DSL has operational responsibility for ensuring that online safeguarding concerns are appropriately identified, assessed and addressed.

The DSL is responsible for:

- Overseeing the safeguarding effectiveness of NetSweeper filtering and monitoring.
- Ensuring monitoring alerts are reviewed and appropriately escalated.
- Assessing concerns in the context of individual pupils' needs and vulnerabilities.
- Recording safeguarding concerns and actions on LearnTrek.
- Liaising with the Proprietors, staff, IT support and external safeguarding agencies.
- Authorising and documenting safeguarding-related filtering decisions.
- Reviewing patterns of online behaviour and emerging risks.
- Supporting staff to understand online safeguarding responsibilities.
- Coordinating termly reviews and the annual in-depth filtering and monitoring review.
- Ensuring arrangements remain appropriate following significant safeguarding incidents or changes in technology.

Where the DSL is unavailable, concerns must be referred to the designated deputy or the safeguarding escalation arrangements set out in the Safeguarding Policy.

5.3 IT Support / Technical Provider

The person or provider responsible for technical support will:

- Maintain the technical configuration of NetSweeper.
- Ensure filtering and monitoring are applied to the intended networks and devices.
- Manage software updates, security settings and access permissions.
- Investigate identified technical weaknesses.
- Support filtering tests and system effectiveness reviews.
- Provide relevant reports and technical information to the DSL.
- Ensure that changes to technology do not unintentionally weaken safeguarding controls.
- Support secure management of monitoring data.

Technical support must not independently determine the safeguarding significance of an incident. Safeguarding decisions remain the responsibility of the DSL and school leadership.

5.4 All Staff

All staff are responsible for promoting online safety and remaining vigilant to potential risks.

Staff must:

- Complete required safeguarding and online safety training.
- Read and comply with the E-Safety Policy and Acceptable Use Agreement.
- Maintain appropriate supervision whenever pupils use digital technology.
- Remain alert to inappropriate content, concerning searches or unsafe online behaviour.
- Report safeguarding concerns immediately to the DSL.
- Record concerns through LearnTrek in accordance with school procedures.
- Never assume that NetSweeper will identify every safeguarding risk.
- Report suspected filtering failures, security breaches or attempts to bypass controls.
- Support pupils to develop safe and responsible online behaviours.

5.5 Pupils

Pupils are supported to:

- Use technology safely and responsibly.
- Follow the school's Acceptable Use Agreement.
- Respect others when communicating online.
- Report content or interactions that make them feel uncomfortable or unsafe.
- Understand that school internet use is subject to filtering and monitoring.
- Develop an understanding of online risks appropriate to their age and individual needs.

Filtering, Monitoring and Technical Controls

TILT Education uses a combination of technical systems, staff supervision and safeguarding procedures to provide a safe online environment.

Filtering and monitoring serve different but complementary purposes.

Filtering seeks to prevent access to illegal, harmful or inappropriate online material.

Monitoring helps identify concerning online activity so that staff can assess the risk and take appropriate safeguarding action.

Both are necessary elements of TILT Education's approach to online safety.

6.1 Use of NetSweeper

TILT Education uses NetSweeper as its web content filtering and monitoring solution.

NetSweeper provides category-based web filtering, reporting and monitoring functionality designed to support schools in managing access to online content and identifying potentially concerning online activity.

NetSweeper's published education product information describes dynamic content categorisation, configurable filtering policies, activity logging, reporting and monitoring. The precise capabilities available to TILT Education depend on the modules purchased and their configuration.



Netsweeper

TILT Education's purchased provision includes monitoring logs and automated alerts, which form part of the school's wider safeguarding arrangements.

The system is used to:

- Restrict access to harmful or inappropriate online content.
- Apply filtering rules to categories of websites and online material.
- Record relevant web activity and attempts to access restricted content.
- Generate alerts where configured risk indicators are identified.
- Provide reports to support safeguarding oversight and technical review.
- Identify recurring concerns or attempts to circumvent filtering controls.
- Inform timely safeguarding interventions where concerns are identified.

NetSweeper alerts are assessed by authorised staff and considered alongside staff observations, individual pupil circumstances and other safeguarding information.

An automated alert does not automatically establish that a pupil has engaged in harmful behaviour. Alerts must be reviewed and interpreted appropriately.

6.2 Content Filtering

TILT Education's filtering arrangements are intended to prevent access to illegal, inappropriate and potentially harmful online material.

Filtering categories include, where relevant:

- Child sexual abuse material.
- Terrorist and extremist content.
- Pornography and sexually explicit material.
- Material promoting self-harm or suicide.
- Gambling and illegal activities.
- Malware, phishing and malicious websites.
- Harmful or discriminatory content.
- Circumvention tools, including unauthorised proxy services and VPNs.

Filtering arrangements will be reviewed to ensure they do not unnecessarily restrict legitimate educational content.

The school will seek assurance from its provider that appropriate arrangements are in place for blocking known child sexual abuse material and unlawful terrorist content, including the use of relevant recognised intelligence sources.

6.3 Filtering Coverage

TILT Education aims to ensure appropriate filtering is applied to all school-managed internet access arrangements, including:

- School internet connections and any backup connections.

- School wireless networks.
- School-owned desktop computers and laptops.
- School-managed tablets and other internet-enabled devices.
- School-owned devices used away from the premises, where technically supported and configured.

The school will maintain a record of which networks and devices are protected and identify any gaps in coverage.

Where a device, application or connection cannot be protected by the existing filtering arrangements, an appropriate risk assessment and alternative safeguards must be implemented.

6.4 Age-Appropriate and SEND-Appropriate Filtering

Filtering arrangements will take account of:

- Pupils' ages and developmental stages.
- Individual SEND needs and vulnerabilities.
- Educational requirements and curriculum access.
- Language and communication needs, including EAL where relevant.
- Emerging risks and changing patterns of internet use.

The DSL will consider whether filtering restrictions are proportionate and effective for the pupils attending TILT Education.

Requests to unblock educational content must be reviewed and authorised by the appropriate member of staff, with safeguarding considerations documented.

6.5 Monitoring and Automated Alerts

NetSweeper supports TILT Education's monitoring arrangements through activity logs, reports and automated alerts.

Depending on the technical configuration, monitoring information may include:

- Device identifiers and IP addresses.
- Named users, where user identification is supported.
- Dates and times of activity.
- Website addresses and relevant browsing activity.
- Search terms or attempted access to restricted content, where captured.
- Filtering categories and triggered alerts.

Monitoring information is used to identify potential safeguarding concerns, including repeated attempts to access harmful material, unsafe browsing activity and attempts to bypass security controls.

Authorised staff must review alerts promptly, assess their significance and take appropriate action.

Monitoring arrangements must be proportionate, lawful and transparent.

6.6 Physical Supervision

Technical monitoring is supplemented by high levels of direct staff supervision.

At TILT Education, pupils are supported by staff when using digital technology, with a minimum supervision ratio of one adult to two pupils in accordance with the school's established practice.

Staff must:

- Remain aware of the websites, applications and digital activities pupils are accessing.
- Position themselves to provide effective supervision.
- Respond immediately when inappropriate content or behaviour is identified.
- Support pupils to understand and manage online risks.
- Report concerns through established safeguarding procedures.

Supervision arrangements may be increased where individual risk assessments or pupil needs require additional support.

6.7 Network and Device Monitoring

TILT Education uses network and device monitoring arrangements to support online safeguarding.

Network monitoring includes reviewing relevant internet activity and access logs.

Device monitoring may include additional software or technical controls where these have been installed and configured.

The school will maintain an accurate record of the monitoring arrangements applied to its devices and networks.

The DSL and technical support will work together to identify any areas where monitoring coverage is incomplete and implement appropriate safeguards.

6.8 SafeSearch and Circumvention Controls

TILT Education will ensure that SafeSearch is enabled and appropriately restricted on school-managed browsers and search engines.

Where technically possible, users will be prevented from:

- Disabling SafeSearch.
- Installing unauthorised browsers or extensions.
- Using VPNs, proxy services or anonymising tools to bypass filtering.
- Altering device settings that could weaken safeguarding controls.
- Accessing unfiltered internet connections through school-managed devices.

Suspected circumvention will be reported to the DSL and technical support.

NetSweeper Alert Management and Safeguarding Response

NetSweeper monitoring alerts form part of TILT Education's established safeguarding procedures.

The DSL is responsible for ensuring that alerts are assessed and that appropriate action is taken.

7.1 Alert Review

- High-risk safeguarding alerts must be brought to the attention of the DSL immediately upon identification.
- NetSweeper monitoring reports will be reviewed at least weekly, with additional checks where risk indicates.
- The DSL will consider the nature of the alert, the pupil's circumstances and any previous safeguarding concerns.

- Relevant alerts and actions will be recorded on LearnTrek.
- Technical concerns will be referred to IT support.
- Patterns or repeated concerns will inform safeguarding reviews and preventative interventions.

The DSL will ensure that suitable arrangements exist for receiving and responding to urgent alerts during school operating hours. Arrangements for alerts outside school hours will be documented according to the school's monitoring service and staffing provision.

7.2 Responding to an Alert

When an alert identifies a potential safeguarding concern, the following process applies:

1. Identify: The alert is received or concerning activity is observed.
2. Assess: The DSL considers the information, context, severity and immediate risk.
3. Act: Appropriate safeguarding action is taken, including pupil support, parental contact or external referral where necessary.
4. Record: The concern, decisions, actions and outcomes are recorded on LearnTrek.
5. Review: The DSL considers whether further monitoring, intervention or technical changes are required.

Where there is an immediate risk of serious harm, staff must follow the school's emergency safeguarding procedures without waiting for a routine monitoring review.

7.3 Reporting to Proprietors

The DSL will provide the Proprietors with termly information about:

- The number and nature of significant online safeguarding concerns.
- NetSweeper alerts requiring safeguarding intervention.
- Recurring risks or concerning patterns.
- Filtering and monitoring effectiveness.
- Technical weaknesses and corrective actions.
- Recommendations for staff training or curriculum development.

Reports will be proportionate and protect pupil confidentiality.

Testing and Reviewing Filtering and Monitoring

TILT Education recognises that filtering and monitoring arrangements must be regularly tested and reviewed to ensure they remain effective.

8.1 Routine Checks

The DSL and technical support will coordinate checks to confirm that:

- NetSweeper is operating as intended.
- Filtering rules are applied to the correct users and devices.
- Monitoring alerts and reports are being generated and received.

- School internet connections remain appropriately protected.
- Safeguarding concerns are being identified and escalated.
- Changes to software or equipment have not reduced protection.

The frequency of technical checks will be informed by the school's risk assessment, with formal effectiveness reviews undertaken termly.

8.2 Filtering Tests

TILT Education will use recognised testing tools, including the South West Grid for Learning (SWGfL) filtering test available at testfiltering.com, to help evaluate filtering effectiveness.

Testing will consider whether access to illegal child sexual abuse material, unlawful terrorist content and adult content is appropriately blocked.

The school will also review the suitability of filtering for pupils with SEND and the availability of appropriate curriculum materials.

8.3 Annual In-Depth Review

The DSL, supported by the Headteacher and technical support, will undertake a documented in-depth review at least once every academic year.

This review will consider:

- The needs and risk profiles of pupils.
- The effectiveness and coverage of NetSweeper.
- Safeguarding alerts and incident records.
- Filtering categories and permitted exceptions.
- SEND accessibility and individual vulnerabilities.
- Emerging risks, including generative AI.
- Changes in technology, devices and internet use.
- Staff training needs.
- Areas requiring improvement.

The findings, actions and outcomes will be recorded and made available to those entitled to inspect them.

8.4 Additional Reviews

Filtering and monitoring arrangements will also be reviewed following:

- A significant safeguarding incident.
- Identification of a technical weakness.
- Introduction of new devices or software.
- Major system or network configuration changes.
- Changes to remote access or bring-your-own-device arrangements.
- Introduction of new AI applications or digital learning platforms.

8.5 Records of Checks

All formal filtering and monitoring checks will be documented.

Records will include:

- Date and time of the check.
- Name of the person completing it.
- Device, system or network tested.
- Nature of the test.
- Findings and identified weaknesses.
- Actions required and person responsible.
- Completion date and confirmation of resolution.

These records will provide evidence of ongoing safeguarding oversight.

Staff Training and Awareness

All staff receive safeguarding and online safety training as part of their induction and ongoing professional development.

Training includes:

- Recognising online safeguarding risks.
- Understanding filtering and monitoring arrangements.
- Reporting online concerns through LearnTrek.
- Recognising grooming, exploitation, radicalisation and cyberbullying.
- Understanding risks associated with artificial intelligence, deepfakes and misinformation.
- Maintaining appropriate supervision of pupils.
- Responding to inappropriate content or unsafe online behaviour.

Staff with responsibility for NetSweeper alerts or monitoring reports will receive additional training appropriate to their roles.

The DSL will undertake enhanced safeguarding training and remain informed about emerging online risks.

Training needs will be reviewed annually and following significant incidents or changes to technology.

10. Educating Pupils About Online Safety

Online safety is incorporated into TILT Education's wider curriculum, including PSHE, computing, life skills and other relevant learning opportunities.

Teaching is differentiated to reflect pupils' individual needs, communication abilities and developmental understanding.

Pupils are supported to develop knowledge and skills in:

- Recognising harmful and inappropriate content.
- Understanding safe and unsafe online relationships.
- Identifying grooming, exploitation and radicalisation.
- Recognising cyberbullying and online harassment.

- Understanding privacy, consent and the sharing of images.
- Evaluating online information critically.
- Identifying misinformation, disinformation and AI-generated content.
- Understanding digital footprints and online reputation.
- Reporting concerns and seeking support.
- Developing resilience and responsible digital behaviours.

Where appropriate, pupils are introduced to trusted reporting services, including CEOP.

Learning activities may include visual resources, practical demonstrations, role-play, supported discussion and real-life scenarios.

Working with Parents and Carers

TILT Education recognises that effective online safeguarding requires cooperation between school and home.

Parents and carers will be supported through:

- Online safety information shared through newsletters and school communications.
- Signposting to trusted safeguarding and online safety resources.
- Guidance on managing internet access and online risks at home.
- Information about emerging risks, including social media, exploitation and AI-generated content.
- Individual discussions where a pupil's online behaviour or vulnerability raises concern.
- Workshops or information sessions where appropriate.

Parents and carers will be informed about the school's filtering and monitoring arrangements through relevant policies and privacy information.

12. Managing Online Safety Incidents

All online safeguarding concerns must be reported immediately to the DSL and recorded in accordance with the school's safeguarding procedures.

Concerns may arise through:

- NetSweeper alerts.
- Staff observations.
- Pupil disclosures.
- Parent or carer reports.
- Monitoring reports.
- Information from external agencies.

The DSL will assess each concern and determine the appropriate response.

Actions may include:

- Providing immediate support to the pupil.

- Implementing safeguarding interventions.
- Contacting parents or carers where appropriate and safe.
- Reviewing individual risk assessments.
- Adjusting supervision arrangements.
- Reviewing filtering and monitoring settings.
- Making referrals to children's social care, police or Prevent services where necessary.
- Considering appropriate behaviour interventions in accordance with school policy.

Safeguarding concerns must not be treated solely as behaviour incidents.

Following significant incidents, the DSL will review whether lessons can be learned and whether changes to policies, technical controls or staff training are required.

Reporting and Recording Through LearnTrek

All safeguarding concerns relating to online safety will be recorded through LearnTrek under the appropriate E-Safety category.

Categories include:

- Cyberbullying.
- Grooming and radicalisation.
- Child sexual abuse material.
- Sexting or harmful sexual behaviour.
- Racist, sexist, homophobic, transphobic or religious hate material.
- Terrorist or extremist content.
- Online gambling or illegal activity.
- Pornography or sexually explicit material.
- Hacking or attempts to bypass security controls.
- Other online safeguarding concerns.

Records should include:

- The date and time of the concern.
- The pupil or pupils involved.
- The nature of the concern.
- Relevant information from NetSweeper, where appropriate.
- Actions taken and staff involved.
- Decisions made by the DSL.
- Referrals or communication with external agencies.

- Outcomes and follow-up actions.

Records must be factual, accurate and handled confidentially.

Where suspected illegal imagery is involved, staff must follow safeguarding procedures and must not unnecessarily view, copy, download or share the material.

Cybersecurity and Data Protection

TILT Education recognises that secure ICT systems are essential to safeguarding pupils, staff and sensitive information.

Appropriate technical and organisational security measures will be maintained.

These include:

- Secure storage of servers, networking equipment and associated infrastructure.
- Restricted physical access to critical ICT equipment.
- Firewalls, antivirus protection and other appropriate security measures.
- Intrusion detection or equivalent protective controls where implemented.
- Secure wireless networks.
- Individual user accounts and passwords.
- Appropriate access permissions.
- Software updates and security patching.
- Protection against malware, phishing and unauthorised access.

14.1 Data Protection and Monitoring

Information collected through NetSweeper will be processed in accordance with the Data Protection Act 2018 and UK GDPR.

Access to monitoring data will be restricted to authorised personnel who require it for safeguarding or technical responsibilities.

TILT Education will ensure that:

- Monitoring is necessary and proportionate.
- Pupils, staff and relevant users are informed about monitoring arrangements.
- A Data Protection Impact Assessment (DPIA) is completed and reviewed as required.
- The provider's privacy and data processing arrangements are reviewed.
- Monitoring information is retained in accordance with the school's approved retention schedule.
- Sensitive safeguarding information is stored and shared securely.
- Automated alerts are subject to appropriate human assessment.

These arrangements reflect DfE guidance on data protection and filtering and monitoring.

Acceptable Use of Technology

All staff and pupils are required to comply with TILT Education's Acceptable Use Agreement.

Agreements will be reviewed and signed annually, with accessible explanations provided to pupils where necessary.

The agreements will explain:

- Expectations for responsible use of school technology.
- Appropriate online behaviour.
- Restrictions on accessing or sharing harmful content.
- The school's filtering and monitoring arrangements.
- Responsibilities for protecting passwords and personal information.
- Procedures for reporting concerns.
- Consequences of deliberate misuse, considered alongside safeguarding needs and individual circumstances.

Staff must not use school technology in ways that compromise safeguarding, confidentiality or data security.

Limitations and Risk Mitigation

TILT Education recognises that no filtering or monitoring system can provide complete protection from online harm.

NetSweeper is one element of a wider safeguarding approach.

The school mitigates remaining risks through:

- High levels of direct staff supervision.
- Individual pupil risk assessments where required.
- Differentiated online safety education.
- Staff vigilance and professional judgement.
- Prompt reporting and investigation of concerns.
- Regular testing and review of technical controls.
- Appropriate parental involvement.
- Continuous improvements to safeguarding procedures.

Where filtering or monitoring weaknesses are identified, TILT Education will assess the associated risks and implement proportionate interim safeguards until the issue is resolved.

17. Monitoring, Review and Continuous Improvement

This policy is subject to ongoing monitoring, refinement and audit by the Proprietors.

The DSL and Headteacher will ensure that online safeguarding arrangements remain appropriate to the needs of pupils and the technology used within the school.

The following review arrangements will apply:

Activity	Frequency	Responsibility
Review urgent safeguarding alerts	Immediately upon identification	DSL / designated safeguarding cover
Review NetSweeper monitoring reports	At least weekly	DSL / authorised staff
Record safeguarding incidents	As concerns arise	All staff / DSL
Filtering and monitoring effectiveness review	Termly	DSL / Headteacher / IT support
In-depth filtering and monitoring review	Annually and following significant changes	DSL / Headteacher / IT support
Staff online safety training review	Annually	DSL / Headteacher
E-Safety Policy review	Annually or sooner where necessary	Proprietors / DSL

Findings from reviews will inform changes to safeguarding practice, staff training, curriculum planning and technical controls.

Appendix A – Technical Filtering and Monitoring Arrangements

A1. NetSweeper Provision

NetSweeper is TILT Education's designated web filtering and monitoring solution.

The school's purchased provision includes web filtering, monitoring logs and automated alerts.

NetSweeper provides tools to support the identification of potentially harmful online activity, reporting and the management of filtering policies.

TILT Education will maintain a technical record confirming:

- The NetSweeper products and modules installed.
- Devices and networks covered.
- Whether off-site filtering and monitoring are enabled.
- Alert categories and notification arrangements.
- Authorised users with access to reports.
- Any identified limitations.
- Technical support and maintenance arrangements.

This record will be reviewed when the service or configuration changes.

A2. Filtering Standards

Filtering arrangements will be assessed against DfE expectations, including:

- Blocking access to known illegal child sexual abuse material and unlawful terrorist content.
- Appropriate implementation of IWF and CTIRU blocklists.
- Age-appropriate and SEND-appropriate filtering.

- Protection against common circumvention techniques.
- Filtering across relevant internet connections and devices.
- Appropriate user profiles for staff and pupils.
- SafeSearch controls.
- Monitoring of attempted access to restricted content.
- Avoiding unreasonable restrictions on legitimate teaching and learning.

Provider assurances and test results will be retained as evidence.

A3. Monitoring Arrangements

TILT Education's monitoring approach combines:

Physical supervision: Staff directly supervise pupils when using technology, maintaining a minimum ratio of one adult to two pupils.

Network monitoring: Relevant web activity and access logs are reviewed through NetSweeper.

Device monitoring: Additional monitoring functionality is used where installed and configured on school-managed devices.

Automated alerts: NetSweeper generates alerts based on configured monitoring rules and identified activity.

Safeguarding response: The DSL reviews concerns, determines appropriate action and ensures relevant information is recorded on LearnTrek.

The school will review whether monitoring arrangements adequately cover browser-based activity, applications and other digital content used by pupils.

A4. Technical Testing

Filtering and monitoring testing will consider:

- Whether prohibited content is appropriately blocked.
- Whether filtering policies apply to the correct user groups.
- Whether monitoring alerts are generated and received.
- Whether reports contain sufficient information to identify and investigate concerns.
- Whether new devices are protected before pupil use.
- Whether changes to networks or software affect protection.
- Whether the system remains appropriate for pupils with SEND.

Testing records will be retained for safeguarding and management review.

A5. Incident and Alert Records

Records of significant monitoring concerns will include:

- Date and time of the alert.
- Nature and severity of the concern.
- Device or user information where available.

- Person reviewing the alert.
- Safeguarding assessment.
- Actions taken.
- LearnTrek reference where relevant.
- Outcome and any further action required.

A6. Technical Limitations

The DSL and technical support will review the limitations of the school's NetSweeper configuration.

This will include whether monitoring can identify risks arising through:

- Mobile applications.
- Messaging services.
- AI-generated content.
- Encrypted or otherwise inaccessible content.
- Devices used outside the school network.
- Alternative internet connections.

Where technical monitoring cannot provide adequate coverage, additional safeguards will be considered.

Appendix B – Filtering and Monitoring Evidence Checklist

The following checklist will support annual reviews and safeguarding audits.

Evidence	Expected record
NetSweeper provision	Contract, modules and configuration details
Filtering coverage	Record of protected networks and devices
Filtering tests	Dated SWGfL test results and actions
Monitoring reports	Weekly review records
High-risk alerts	Evidence of prompt review and response
Safeguarding incidents	LearnTrek records
Technical checks	Testing logs and corrective actions
SEND considerations	Relevant risk assessments and filtering review
Staff training	Training records
Acceptable Use Agreements	Annual signed agreements
Data protection	DPIA and relevant privacy notices
Termly reviews	Recorded findings and actions
Annual review	Completed filtering and monitoring review