TRUST IN LEARNING (ACADEMIES)

Online Safety Policy

Approval Date: November 2025	Version: 01	Review: 1 year (or sooner if required by statutory guidance)
Approval By: Quality of Education Committee	Lead: Director of School Improvement, Chief Financial Officer	Review date: Autumn 2026
As part of the review process, this policy/procedure has been subject to an Equality Impact Assessment.		

History of Policy Changes:

Date	Page	Change	Reason for Change
September 2025		New policy	New over-arching policy for the Trust

Contents

1. Statement of Intent

This document sets out the policy for Online Safety within Trust in Learning Academies (the Trust).

The policy has been developed and implemented in consultation with schools.

2. Values and Principles

This Trust Policy is set out with the following principles at its core:

Trust in Learning Academies is a family of schools each with a distinctive identity, collaborating to strengthen and support each other. We deliver high quality education with evidence-informed approaches to teaching, learning and the curriculum. Inclusion is at the heart of all we do. We actively listen to the voices of our pupils, staff and communities. Every school makes deliberate choices to be sustainable and globally focused.

The Trust vision is to:

- Inspire pupils to trust in learning and achieve their full potential
- To empower pupils to have confidence in their successes to make a positive contribution to the world
- To remove barriers to learning and help transform the lives of our pupils

Any data collected, stored or managed as a result of this policy is in accordance with UK and any relevant retained or assimilated EU law, and in line with the Trust's ethos and values.

This Policy has been framed in accordance with the guidance on best practice from the Department for Education (DfE).

3. Objectives and Scope

3.1 The specific aims of this policy are to:

- Outline the Trust's approach to online safety which empowers schools to protect and education the school community in its use of technology.
- Ensure robust processes are in place to safeguard pupils, staff and volunteers
- Ensure that pupils who are more vulnerable to harm online are effectively identified and supported

3.2 This policy has due regard to legislation and statutory guidance, including but not limited to, the following:

- Education Act 1996 and 2011;
- Equality Act 2010;
- Education and Inspections Act (2006);
- DfE (2025) Keeping children safe in education (KCSIE);
- National Curriculum computing programmes of study

3.3 This policy will be implemented in conjunction with the following Trust policies:

- Artificial Intelligence Policy
- Anti-bullying Policy
- Behaviour Policy

- Code of Conduct Policy
- Data Protection and GDPR Policy
- Safeguarding and Child Protection Policy
- Special Educational Needs and Disability Policy

4. Responsibilities and Accountabilities

4.1 Responsibilities of the Trust Central Education Team

- To ensure that the policy, as written, does not discriminate on any grounds, including, but not limited to, age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.
- To ensure the policy is well communicated to all Headteachers.
- To ensure that the policy is regularly reviewed.

4.2 Responsibilities of the Headteacher

- To ensure the implementation of and compliance with current policy and procedures at school level
- To monitor systems, resources, impact and actions related to the policy
- To ensure the policy is well communicated and staff understand their role in its implementation
- To handle any complaints at school level which arise through this policy

4.3 Responsibilities of the Designated Safeguarding Lead (DSL)

- To take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies/documents
- To work with Central ICT Team to ensure appropriate filtering and monitoring systems are in place
- To keep stake holders up to date with relevant online safety information and provide regular training
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- To liaise with the Local Authority/MAT/other external agencies as required
- To liaise with school technical staff
- To receive reports of online safety incidents, log incidents on CPOMS and respond to any safeguarding concerns
- Regularly analyse online safety incident reports to identify trends in concerns, implementing an appropriate strategic response
- To report regularly to Senior Leadership Team
- To undertake necessary online safety training so that they are aware of the potential for serious child protection/safeguarding issues to arise from online incidents
- Each year, to review online safety procedures and risk assess accordingly.

4.4 Responsibilities of the Trust Central IT Team:

- To put in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school.
- To make sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- To regularly conduct a full security check and monitoring the school's ICT systems

- To block access to potentially dangerous sites and, where possible, prevent the downloading of potentially dangerous files
- To make sure that any online safety incidents are logged and dealt with appropriately in line with this policy.

4.5 Responsibilities of general school leadership

- To ensure staff are inducted into the procedures surrounding this policy and any updates
- To provide training to ensure policy compliance
- To hold sessions for parents and pupils as required, to ensure the policy is understood

4.6 Responsibilities of all staff

- To uphold the whole school approach to the policy through modelling expected standards and utilising appropriate school procedures, including safeguarding and acceptable use procedures.
- To keep up to date with policy changes over time
- To promote a collaborative and inclusive ethos where all pupils can thrive
- To feed back to school leaders where concerns may arise in the implementation of the policy

4.7 Responsibilities of parents

- To support the implementation of the policy with their child, as appropriate
- Where a parent has feedback on the implementation of the policy, to raise this directly with the school while continuing to work in partnership with the school

4.8 Responsibilities of pupils

- To uphold school rules and expectations and thereby comply with the implementation of the policy, including acceptable use procedures
- To feed back on the implementation of the policy through appropriate means, such as school council, to school staff

5. Online Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content**: being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact**: being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and/or financial scams

5.1 Assessment of risk

Each year, schools should review online safeguarding procedures to ensure that they remain robust and in line with statutory guidance. An online safety risk assessment should be completed to identify online safety risks and mitigations implemented by school.

5.2 Reporting concerns around online safety

Any safeguarding concerns around online safety should be reported following the school's safeguarding reporting procedures. These are outlined in the Safeguarding and Child Protection Policy.

6. Educating Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety and digital literacy is an essential part of TILA's online safety provision.

Online safety is a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum, in line with the National Curriculum. Online safety is also delivered through discrete lessons such as computing/PSHE as well as through whole school assemblies and tutorial/pastoral activities.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

7. Partnership with Parents

To effectively educate and safeguard pupils from online safety risks, partnership with parents/carers is crucial.

To raise the profile of online safety, and to support parent/carers in keeping up to date with developments, the school will keep online safety high profile with parents/carers through:

- regular letters/emails home, raising awareness of online safety and signposting to relevant resources
- information via the school website
- information shared through parents' evenings
- online safety workshops for parents.

In line with Trust Policy, if parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

8. Cyber Bullying

Bullying is the **repetitive**, **intentional hurting** of one person or group by another person or group, where the relationship involves an **imbalance of power**. Bullying can be **physical, verbal or emotional/psychological**. (Anti-Bullying Alliance, 2024)

It can involve people of any age, and can happen anywhere – at home, school or using online platforms and technologies (cyberbullying). This means it can happen at any time.

Cyber bullying is a form of bullying. Examples of cyber bullying include:

Cyber bullying/online abuse e.g.

- excluding a child from online games, activities or friendship groups
- sending threatening, upsetting or abusive messages
- creating and sharing embarrassing or malicious images or videos
- 'trolling' - sending menacing or upsetting messages on social networks, chat rooms or online games
- voting for or against someone in an abusive poll
- setting up hate sites or groups about a particular child
- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name.

As a school we acknowledge our responsibilities to investigate and support families if bullying occurs off the premises. The school reserves the right to discipline for behaviour off the premises, where incidents impact on relationships within school.

The Trust's approach to prevent and respond to any incident of bullying, including cyber bullying, is outlined in the Anti-Bullying Policy. The school's procedures to prevent, and in response to incidents of cyber bullying, are outlined in the school's ***Online Safety Procedures***. Both are available on the school website.

8.1 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- poses a risk to staff or pupils, and/or
- is identified in the school rules as a banned item for which a search can be carried out, and/or
- is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher/DSL
- explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- cause harm, and/or
- undermine the safe environment of the school or disrupt teaching, and/or
- commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL/Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **not** view the image
- confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with TILA's Behaviour Policy, which follows the latest DfE guidance on searching, screening and confiscation .

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the TILA's Complaint's Policy.

9. Use of Artificial Intelligence (AI)

Generative AI tools are now widespread and easy to access. TILA recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others.

TILA's approach to the use of AI is detailed in the AI Policy.

10. Acceptable use of the internet in school

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with this policy and restrict access through filtering systems where appropriate.

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (included in the Annex). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

11. Pupil use of mobile phones

TILA understands the value of access to the internet but recognises the growing body of evidence that smartphones negatively affect children's physical and emotional wellbeing, their learning, and expose them to serious safeguarding risks. Smartphones are designed to be highly addictive, and excessive screen time can reduce opportunities for play, social interaction, and creative exploration. Research increasingly links smartphone use in children to:

- lower self-esteem, anxiety, and depression
- impaired attention and focus
- sleep deprivation
- loneliness and reduced social interaction
- cyberbullying, grooming, and exposure to misogynistic or pornographic content.

The Trust recommends that parents consider delaying their child's first smartphone until at least the age of 14. The objective of this is:

- to encourage more play,
- strengthen face-to-face friendships,
- support more effective learning,
- improve physical and mental health,
- reduce children's exposure to online harm.

If children do have smartphones, the Trust suggests that parents remove the web browser and app store to limit access to harmful content and addictive apps. If pupils need to communicate with parents on their way to and from school, parents should consider a basic phone with no internet access.

TILA secondary schools have a ban on smartphone usage during the school day, using Yondr pouches to enforce this.

School procedures for mobile phone usage are detailed within the school's Online Safety Procedures.

12. Staff use of work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Updating anti-virus and anti-spyware software as required

- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in the Online Safety Policy Annex.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Central IT.

13. School response to issues of misuse

Where a pupil misuses the school's ICT systems or internet, the school will follow the process set out in their behaviour procedures. Where necessary, an appropriate safeguarding response may also be required. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct. Action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

14. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

As part of safeguarding training, all staff members will receive online safety refresher training at least once each academic year as well as relevant updates through the year as required.

The DSL training, which is renewed every two years, includes online safety. The DSL will ensure that they update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Appendix 1: Online Safety School Procedure guidance

Each school must have online safety procedures documented and reviewed annually. These should be saved on your website and should include an outline of the following:

1. Online Safety Curriculum
2. Approach to educating parents/carers about online safety
3. School expectations on the use of mobile phones
4. School procedures to prevent and respond to cyber-bullying (linking with anti-bullying procedures)