TEAM
Multi-Academy Trust

E-Safety Policy 2025

This Policy was adopted by the TEAM Multi-Academy Trust Board of Trustees on

Date: 6th October 2025

Signed: Sue Wells (on behalf of the Board of Trustees)

Signed: Ian Thomas (Trust Chief Executive Officer)

Reviewed: Oct 2025

Next Review Due: Autumn 2027

1. Aims

- Have robust processes in place to ensure the online safety of pupils, staff, Trustees, Governors and volunteers.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, record, intervene and escalate an incident, where appropriate.
- Equip pupils, staff and parents with the knowledge and tools needed to identify risks such as online grooming, disinformation, AI-generated content, and image-based abuse.

2. Legislation and guidance

- This policy is based on the Department for Education's statutory safeguarding guidance: *Keeping Children Safe in Education (2025)*,
- and non-statutory guidance such as *Teaching Online Safety in Schools (2024)* and *Filtering and Monitoring Standards (2023)*.
- It reflects relevant legislation, including: the Education Acts 1996, 2006, and 2011; the Equality Act 2010; and the Prevent Duty.
- The Trust also complies with the General Data Protection Regulation (GDPR), Data Protection Act 2018, and guidance from the UK Safer Internet Centre.

3. Roles and responsibilities

- The Board of Trustees oversees implementation and reviews updates, meeting termly to monitor the DSL's logs and incident reports.
- The CEO ensures consistent implementation and resourcing across schools. The CEO, or Director of Education (DoE) in the absence of the CEO, follows up on any serious online safety incidents with the relevant Head of School.
- The DDSL leads in each school and the Trust DSL lead on online safety and safeguarding, delivers staff training, logs incidents, and liaises with external agencies when appropriate.
- The CEO liaises with the Trust's appointed external IT consultant to ensure robust filtering and monitoring systems aligned with the DfE's 2023 standards and performs monthly audits.
- The CEO, Heads of School, and IT consultant receive daily and weekly reports from Smoothwall, and serious incidents are flagged and escalated promptly.
- All staff must implement the Acceptable Use Policy (AUP), model safe online behaviour, and log/report any incidents promptly.
- Parents must sign the AUP, promote safe online behaviours at home, and raise concerns with the DSL or Head of School.

4. Educating pupils about online safety

- Online safety is embedded in the computing and PSHE curriculum from EYFS to Year 6.
- The Trust uses the *Jigsaw* PSHE scheme, which includes age-appropriate content on:

    - Responsible internet use and reporting concerns.
    - Privacy, online reputation, and digital footprint.
    - Recognising online scams, grooming, and fake news.
    - Safe and critical use of AI tools and awareness of synthetic content (e.g. deepfakes).
      • The curriculum is reviewed regularly to ensure it reflects emerging risks and technologies.

5. Educating parents about online safety

- The Trust supports parents through regular newsletters, online safety workshops, guidance on filtering tools, and links to UKSIC and CEOP resources.
- Parents receive information during induction and parent-teacher meetings, and are encouraged to engage with home learning platforms safely.

6. Cyber-bullying

- Cyber-bullying is defined as repeated, intentional harm conducted via digital means, including messaging apps, social media, or gaming platforms.
- The Trust addresses this through PSHE, staff training, pupil workshops, and parent guides.
- Incidents are logged, investigated by the school DDSL and Trust DSL, and may be escalated to the police if illegal content is involved.
- Trust staff have powers under the Education Act 2011 to search and delete inappropriate content from devices with 'good reason' following advice and support from DSL and IT consultant.

7. Acceptable use of the internet in school

- All pupils, staff, governors, and volunteers must sign to confirm they have read the Acceptable Use Agreement (AUA) annually.
- School internet access is filtered and monitored using *Smoothwall* for safeguarding compliance.
- Pupils in our primary schools have limited access to AI tools. Where AI tools are used, they must be explicitly approved by the Director of Education and used under direct teacher supervision for educational purposes only.
- Non-educational use of the internet is prohibited unless explicitly authorised.

8. Pupils using mobile devices in school

- Mobile phones are not allowed unless authorised by the Head of School in writing.
- Devices must be handed to the office for safekeeping and use is prohibited during the school day.
- The Trust accepts no responsibility for lost or damaged personal devices.

9. Staff using work devices outside school

- Staff must ensure work devices are password-protected and used solely for work purposes.
- No unauthorised software or personal use is allowed.
- Staff must report any data breaches or suspected device loss immediately to the Trust Link Data Protection Officer (LDPO) and IT consultant.

10. How the school will respond to issues of misuse

- Incidents involving pupils will follow the Behaviour Policy, with sanctions proportionate to severity.
- Staff misuse is handled under the Disciplinary Policy and may involve external reporting where necessary.
- Illegal content is always referred to the police and/or LADO as required.

Parent engagement and conduct
Parents and carers are expected to support the Trust's approach to online safety by modelling respectful digital behaviour and following the Trust's Parent and Carer Code of Conduct. This includes using social media responsibly and raising concerns through the appropriate channels. Where breaches of the Code of Conduct involve digital platforms, online harassment, or unauthorised recordings, they will be escalated in line with the Managing Unreasonable Parent and Carer Behaviour Policy and, where necessary, restricted access procedures may apply.

11. Training

- All new staff receive online safety training during induction.
- Annual refresher training is delivered to all staff, with additional updates shared via newsletters and briefings.
- DSL and deputies undergo enhanced safeguarding training every two years and remain up to date annually.
- Trustees are trained in digital safeguarding as part of their statutory duties.

12. Monitoring arrangements

- D/DSLs log all incidents related to online safety and cyber-bullying using the Trust's digital safeguarding system.
- Smoothwall filtering and monitoring systems are audited termly by the ICT Manager.
- The CEO (DoE in CEO's absence), Heads of School, and IT consultant receive daily and weekly automated incident reports. Serious incidents are flagged and escalated, and reports are reviewed with Trustees termly.
- This policy is reviewed every two years or sooner if significant changes arise, and ratified by the Board of Trustees.

13. Asset disposal

- All devices are logged in inventory and securely wiped or destroyed before disposal.
- The Trust complies with Waste Electrical and Electronic Equipment (WEEE) regulations and data protection laws.
- A certificate of disposal is obtained from the authorised recycling agency.

14. Inclusion and Accessibility

- The Trust ensures online safety education is inclusive of all pupils.
- For pupils with SEND, this includes the use of social stories, visual prompts, simplified language, and one-to-one discussions where necessary.
- Staff will differentiate lessons and provide extra scaffolding where needed to ensure understanding and safety for all learners.

15. Incident Thresholds and Escalation

- Minor incidents (e.g. accidental access to blocked content) are logged and addressed with a conversation and reminder of expectations.
- Moderate incidents (e.g. repeated breaches, unkind messages) involve parental contact and follow-up monitoring.
- Serious incidents (e.g. illegal content, image sharing, grooming, radicalisation) are referred to the DSL immediately and may involve external agencies such as police or LADO.
- Where AI tools are misused to generate inappropriate, misleading, or harmful content, this will be treated in line with the thresholds above and escalated accordingly.

16. Pupil Participation and Voice

- Pupils are involved in promoting online safety through School Councils, Digital Leader roles, or E-Safety Ambassadors.
- These pupils may help shape curriculum content, lead assemblies, and support campaigns such as Safer Internet Day.

- Feedback is also gathered from pupils through surveys or class discussions to evaluate the impact of online safety education.

17. Annual Audit and Action Plan

- Each school within the Trust will complete an annual Online Safety Audit coordinated by the DSL, IT consultant and other key members of staff.
- Findings will inform a localised Online Safety Action Plan to improve provision, systems, and training.
- The Board of Trustees will receive a summary of Trust-wide audit findings and key priorities each spring term.

18. Glossary of Online Safety Terms

- **AI (Artificial Intelligence):** Technology that simulates human intelligence. Can generate content such as text, images, or videos.
- **Deepfake:** AI-generated video or audio designed to mimic real people, often used to mislead or manipulate.
- **Disinformation:** False or misleading information spread deliberately.
- **Doxxing:** The act of publicly revealing private personal information online without consent.
- **Filtering:** Software that restricts access to inappropriate or harmful content on the internet.
- **Grooming:** Building an emotional connection with a child online to exploit or abuse them.
- **Misinformation:** Inaccurate or misleading information shared without malicious intent.
- **Phishing:** Attempt to obtain sensitive information by pretending to be a trustworthy source.
- **AI Hallucination:** When an AI tool generates inaccurate or misleading information that appears factual.
- **Generative AI:** AI tools that create new content, such as written text, images, or video.

19. Links with other policies

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- Remote Learning Policy
- Parent Code of Conduct
- Managing Unreasonable Parents Policy
- Trust AI Policy