Online Safety Guidance

Document Control

Date	Revision amendment details	By whom
May 2022	Approved by TEFAT Board	Trustees
May 2025	Review subject to any required statutory updates	Ops Group
May 2026	Regular review	Ops Group

Table of contents

Related policies and documents

- TEFAT Safeguarding and Child Protection Policy, September 2025
- Keeping Children Safe In Education, (KCSIE) September 2025
- *Working Together to Safeguard Children, March 2026*
- Teaching Online Safety in School - DfE June 2019 to be read in conjunction with:
- Education for a Connected World Framework - UKCIS, 2018.
- The use of social media for online radicalisation, July 2015
- Protecting children from radicalisation, The Prevent Duty, October 2022
- Trust related policies including: Whistleblowing, Allegations Against A Staff Member,
- IT and Internet Acceptable Use and Online Safety
- Teaching online safety in schools, 2019
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships, sex and health education, guides for schools DfE, Updated Sept 21
- Searching, screening and confiscation, updated 2023
- 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' , March 2024
- TEFAT Interim AI Guidance on the use of AI in schools
- Generative Artificial intelligence (AI) in education, August 2025

Definitions

- Where the word 'Trust' is used in this document it refers to The Elliot Foundation Academies Trust, the responsible body
- Where the word 'Principal' is used it refers to the school leader of an individual academy and/or federated academy within the Trust.
- Where the word 'Parent' is used in this document it refers to all those with parental responsibility, including guardians and carers.
- Where appropriate an individual school will make available details of the locally owned procedures and practices to support the implementation of Trust policies.
- Where the title Chair of the Board of Trustees is used it refers to the Chair of the Trust, this being Davie Gallie, who can be contacted via office@elliotfoundation.co.uk.
- Where the abbreviation CEO is used it refers to The Chief Executive Officer of the Trust, this being Hugh Greenway: hugh.greenway@elliotfoundation.co.uk
- Where the Trust Designated Safeguarding Lead (DSL) is used, it refers to the named person in the Trust Safeguarding and Child Protection Policy. This being Caroline Oliver: caroline.oliver@elliotfoundation.co.uk and Deputy DSL being Travis Latham: travis.latham@elliotfoundation.co.uk

Elliot Foundation Academies Trust Values

1. Put children first

a. We trust and value your professionalism
b. We share the responsibility for the learning and welfare of all of our children
c. Our purpose is to improve the lives of children

2. Be safe

a. Don’t assume that someone else will do it
b. Look after yourself, your colleagues and all children
c. We are all responsible for each other’s safety and well being
d. Discuss any concerns with an appropriate member of staff

3. Be kind & respect all

a. People are allowed to be different as are you
b. Kindness creates the positive environment we all need to flourish
c. This kindness should extend to ourselves as well as to others

4. Be open

a. If you can see a better way, suggest it
b. If someone else suggests a better way to you, consider it
c. We exist to nurture innovators and support those who take informed risks in the interests of children

5. Forgive

a. We all make mistakes
b. Admit them, learn from them and move on

6. Make a difference

a. Making the world a better place starts with you
b. Model the behaviour that you would like to see from others

1. Policy statement and objectives

1.1. The Trust and its constituent academies fully recognise our legal responsibilities for safeguarding children in the digital environment, as set out in the policy legal framework above. Safeguarding is paramount and we will always act in the best interests of the child. We aim to create and maintain a culture of vigilance.

1.2. We are committed to safeguarding children and young people and we expect everyone who works in our academies to share this commitment. This policy is in accordance with the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools.

1.3. This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

1.4. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

1.5. The Trust's Online Safety policy applies to all members of our school communities who have access to or use our digital systems, whilst on or outside of school premises.

1.6. This policy will be reviewed every x 3 years or earlier where required as a result of change in the statutory framework; changes in systems or if there are new identified potential threats/risks as technology develops.

The objectives of this policy are to:

- Support our academies to deliver an effective approach to online safety, which empowers us to educate the whole school community in its use of technology and teaches children to make informed choices
- Set clear expectations of behaviour relevant to the responsible use of technology such as the internet for educational, personal or recreational use
- Provide a clear framework for academies to develop and implement their online safety procedures in accordance with this policy
- Ensure that there are effective mechanisms in place to identify, intervene and escalate an incident where appropriate

- Assist staff to work safely and responsibly and to monitor their own standards and practices
- Ensure that all members of the academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- To set out responsibilities of various stakeholders
- Support the Trust's overall aim to create and maintain a safe learning environment where all children and adults feel safe and valued and know they will be listened to and taken seriously

2. Principles

Principles underpinning the aims:

- The welfare of the child is paramount; safeguarding is everyone's responsibility
- It is the responsibility of all adults who work with children to safeguard and promote the welfare of children and to take action where children are at risk from harm
- Staff are responsible for their own actions and behaviour and should avoid any conduct which might lead any reasonable person to question their motivation and intentions
- The same professional standards should be applied regardless of culture, gender, language, disability, racial origin, religious belief and/or sexual identity
- Academies and staff should continually monitor and review their practice in the light of this policy, taking particular care to ensure that all areas are addressed
- Academies must minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

3. Roles and Responsibilities

3.1. **The Trust will:**

- Monitor academy online safety for adults and children through 'Lightspeed' monitoring software and hold regular meetings with the Principal and Designated Safeguarding Lead (DSL) to discuss online safety.
- Regularly review the effectiveness of filtering and monitoring systems against the DfE Filtering and Monitoring Standards.
- Take appropriate steps to ensure the security of the Trust and academy information systems, aligning with the DfE Cyber Security Standards for Schools and Colleges and utilising National Cyber Security Centre (NCSC) training and guidance to strengthen cyber resilience.
- Provide additional AI guidance, ensuring schools use only approved AI tools or aligning with the DfE Generative AI Product Safety Expectations.

- Provide ongoing support for online safety patterns and trends within individual academies, regions and across the whole Trust
- Ensure there are clear and effective escalation routes for raising concerns regarding adults as outlined in the TEFAT Safeguarding and Child Protection Policy, September 2025
- Support the Principal to liaise with the Local Authority Designated Officer (LADO/DO) regarding online/ device allegations against adult/s in school
- Liaise directly with the LADO/DO regarding online/device allegations against adults within the Head Office Team and/or Trustees
- Support the Principal, the Lead and Deputy DSL regarding escalation of child protection/safeguarding issues relating to online use.
- Request assurance that filtering and monitoring responsibilities are understood and tested in practice, rather than just relying on the software's presence.
- Ensure regular safeguarding/online training for Trustees to equip them to provide strategic challenge on policy and monitoring effectiveness, as outlined in KCSIE.

3.2. **The Principal will:**

- Take overall responsibility for online safety provision, data and data security
- Be responsible for ensuring that staff, visitors, volunteers and supply staff understand this policy, and that it is being implemented consistently throughout the school
- Ensure the academy uses an approved, filtered internet service, which complies with current statutory requirements; which is updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant
- Be aware of procedures to be followed in the event of a serious online safety incident and what to do where there is an allegation against a member of staff
- Ensure the SLT receive regular monitoring reports from the Online safety lead to ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager)
- Ensure that any online safety incidents are logged using My Concern, including reports from Lightspeed and dealt with appropriately in line with this policy
- Review the safety and data privacy of Generative AI tools before they are approved for classroom use.
- Ensure pupils will be taught to critically evaluate AI-generated content for accuracy, bias, and potential hallucination.
- Ensure that any incidents of cyber-bullying and/or online child on child abuse are dealt with appropriately in line with the school Safeguarding Policy and Behaviour Policy
- Ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date

- Ensure the security of the academy ICT system e.g. that access controls / encryption exists to protect personal and sensitive information held on academy-owned devices
- Ensure all data held on staff and pupils is held in line with Trust policy and GDPR policy/regulations

This list is not intended to be exhaustive.

3.3. **The Online Safety Lead and/or Designated Safeguarding Lead will:**

- Take day to day responsibility for online safety issues and have a leading role in monitoring compliance with TEFAT online policy and guidance
- Promote an awareness and commitment to online safeguarding throughout the academy community
- Ensure that online safety education is embedded across the curriculum
- Update and deliver staff training on online safety (utilising Flick learning modules)
- Communicate regularly with Regional Innovation Leads, school leaders and the Trust to discuss current issues, review incident logs and filtering
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident raised by Lightspeed or internally
- Ensure that any online safety incident is recorded in MyConcern
- Maintain up to date professional knowledge about Google tools, online safety issues and legislation and the links to child protection or safeguarding concerns
- Ensure that Artificial Intelligence (AI) tools and their associated safety implications are addressed within online safety education and staff training programs.
- Be aware of the potential for serious child protection issues to arise from online access sharing and the sharing of personal data.
- Conduct an annual review of filtering and monitoring logs to identify trends and ensure the system remains effective.

3.4. **All staff, including supply staff, contractors and volunteers will:**

- Maintain an understanding of this policy and implement this policy consistently
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet as shared through locally owned Acceptable Use Agreements
- Supervising and guiding pupils carefully when engaged in learning activities involving online technology and ensuring that pupils follow the school's terms on acceptable use
- Embedding online safety issues in all aspects of the curriculum and other academy activities

- Having an awareness of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current academy policies with regard to these devices.
- Never use personal devices, including the use of Meta smart/AI glasses, to take, store, or transmit images of pupils.
- Reporting any suspected misuse or problem to the DSL (pupils) to the Principal (adults) in line with TEFAT Safeguarding and Child Protection Policy
- Modelling safe, responsible and professional behaviours in their own use of technology
- Ensuring that any digital communications with pupils should be on a professional level and only through academy based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
- Working with the DSL to ensure that any online safety incidents are logged on MyConcern and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying and or online child on child abuse are dealt with appropriately in line with the school safeguarding and behaviour policy

This list is not intended to be exhaustive.

3.5. Parents will:

- Work alongside school to ensure that children understand the importance of using the internet and devices in a safe way
- Ensure their child has read, understood and agreed to the terms of the Pupil Acceptable Use Agreement supporting acceptable use of the school's ICT systems and internet
- Support the academy in promoting online safety and endorse the Parent/Carer Acceptable Use Agreement which includes the pupils' use of the internet and the academy's use of photographic and video images
- Notify a member of staff or the Principal of any concerns or queries regarding this policy or their children's use of technology

3.6. Pupils are expected to:

- Read, understand, sign and adhere to the Pupil Acceptable Use Agreement (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils in addition to pupils agreeing to it within their classroom environment)
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when online
- Know and understand academy policy on the use of mobile phones, digital cameras and handheld devices
- Know and understand academy policy on the taking/use of images, on cyber-bullying and child on child abuse
- Understand the importance of adopting good online safety practice when using digital technologies out of academy

- Realise that the academy's Online Safety Policy covers their actions out of the academy, if related to their membership of the academy
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in the academy and at home

4. Potential Online Risks

4.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and pupils need to be aware of the risks associated with publishing digital images, videos and/or opinions on the internet. Such images and/or comments may provide avenues for cyber bullying and/or peer on peer abuse to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is important that we work together to educate our staff, children, parents and carers to recognise the risks online in an ever changing and evolving online world.

4.2. The risks posed by online activity are a major safeguarding risk to children and must be taken seriously. The main areas of risk can be summarised as follows:

- **Content:**
  Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse, lifestyle websites, e.g. pro anorexia/self harm/suicide sites, hate sites, content validation: how to check authenticity and accuracy of online content, misinformation, disinformation (including fake news), and conspiracy theories.
- **Contact:**
  Grooming, cyberbullying in all forms, identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords;
- **Conduct:**
  Privacy issues, including disclosure of personal information, digital footprint and online reputation, health and wellbeing (amount of time spent online, whether internet or gaming), copyright (little care or consideration for intellectual property and ownership – such as music and film), 'deepfakes" and AI-generated non-consensual imagery. Sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images), sending unsolicited sexual images (Cyberflashing) both of which are illegal and prohibited under the Online Safety Act 2023.
- **Commercialism:**
  Young people's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications. Also, tactics used by apps/influencers to pressure pupils

into spending or sharing data

4.3. When children use the school's network to access the internet, they are protected from inappropriate content by our filtering and monitoring systems. However, many pupils are able to access the internet using their own devices and other networks. To minimise inappropriate use, as a school we use Lightspeed monitoring software which raises alerts directly to the DSLs in school

4.4. Academies ensure their curriculum teaches children how to stay safe online and to be critically aware when online.

4.5. All staff should seek guidance from 'Teaching Online Safety in School' DfE June 2019 to be read in conjunction with Education for a Connected World Framework which offers 'age specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives.

4.6. The Online Safety leader must take responsibility for promoting online safety inside and outside the academy. This may be the DSL or an additional member of staff.

5. Staff Conduct

5.1. Staff are expected to adopt a high standard of personal conduct in order to maintain the confidence and respect of colleagues, children and parents.

5.2. Staff should be aware that safe practice also involves using judgement and integrity about behaviour in places other than work, including online.

5.3. Children face safeguarding risks in exploring the digital world. Staff should adopt responsible online behaviour and must not make contact with children or their families through anything other than official academy accounts.

5.4. No child and/or parent should be in or invited into the home of a member of staff either virtually or physically.

5.5. Staff use of personal mobile phones or cameras is not permitted at any time when children are present (except in emergencies). Staff must not use personal phones for contacting children or parents/carers.

5.6. Any giving of gifts and rewards should only be part of an agreed policy for supporting positive behaviour in school, and should be part of an agreed plan sanctioned by the Principal or a senior member of staff with delegated responsibility.

6. Data Protection, Confidentiality and Information Sharing

6.1. Personal data will be recorded, processed, transferred and made available according to the data protection legislation as detailed in the Trust-wide Data Protection Policy.

6.2. The Trust will only retain the minimum information for as long as necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. More information on retention of data is detailed in the Trust-wide Data Protection Policy.

6.3. To provide parents, staff and pupils with information on how the Trust looks after their data and what their rights are (see Privacy Notices on the Trust website here).

6.4. Undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.

6.5. The Trust's Freedom of Information (FOI) Policy outlines how the Trust manages FOI requests.

6.6. Staff use of personal external storage devices such as USB memory sticks are prohibited. Staff must ensure school supplied devices containing personal data must be encrypted and password protected.

6.7. Staff will receive the appropriate training relevant to their role and any further specific training as required.

7. Equal Opportunities

7.1. The Equality and Diversity Policy sets out the Trust's commitment to tackling disadvantage and discrimination and is implemented locally in school. Leaders must guard against any assumptions about cultural variation where this may be in conflict with safeguarding children when online e.g. FGM and ensure that practices reflect this commitment.

8. Monitoring and Review

8.1. All staff are expected to monitor their own conduct and relationship with children to ensure that the standards expected of them are maintained.

8.2. The Designated Senior Lead will work with the Deputy DSL to monitor the working of the policy and will report as required to the Principal and to the Trust through the annual Trust Safeguarding Audit, Safeguarding national and regional meetings, Regional Director visits and Peer to Peer safeguarding audits.

8.3. The Principal will report to the Trust annually on the working of the policy through the annual Trust Safeguarding Audit.

8.4. RM filtering services support off-site filtering through RM SafetyNet Go. On-site filtering is arranged directly by the school. Lightspeed provides the Trust and academy with regular reports on online safety concerns to ensure pupils and adults are safeguarded.

8.5. TEFAT Regional Innovation Leads provide regular support, training and risk mitigation guidance across the Trust.