Triumph Learning Trust

Aspiration - Collaboration - Innovation

Online Safety Policy

Policy Details

Policy Level	Trust
Document Approver	Trust Board
Document Status	Draft
Applicable to	All Trust Employees
Review Frequency	Every 3 Years

Revision History

Revision	Date	Details	Approved by
0	October 2025	First Issue	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (referred to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key 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, fake news, misinformation and disinformation, 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 them 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, in-content purchasing, phishing and/or financial scams

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation. 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. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyberbullying 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. In the event that files or data on a device may place a child or other person at risk of harm, the school will seek advice from external agencies including the police and children's services. This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will co-ordinate termly meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND).

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding leads

Details of the school's designated safeguarding lead (DSL) [and deputy DSL] are set out in our child protection and safeguarding policy as well as relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on cpoms and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on cpoms and dealt with appropriately in line with the school relational behaviour policy

- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing termly reports on online safety in school to the headteacher and/or governing board

The ICT manager

The school's internet filtering is forced, if it stops working, the Internet would also stop thus protecting the school. We have a firewall in place and the system '**Securely**' to monitor and restrict children's access to inappropriate material online. The ICT manager (SAVVY representative) is responsible for:

- Ensuring security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a termly basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that virus and malware protection and safety mechanisms are reviewed termly
- Conducting a termly security check of the server the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use (appendices 1)
- Working with the DSL to ensure that any online safety incidents are logged on cpoms and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school relational behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites UK Safer Internet Centre, Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behavior
- Identify a range of ways to report concerns about content and contact By the **end of primary school**, pupils will know:
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

.

5. Education Parents about Online Safety

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school relational behaviour policy.)

6. Cyber-Bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school relational behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. All staff and governors receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyberbullying, the school will follow the processes set out in the school relational behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

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

Authorised staff members may examine, 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 DSL / headteacher / other member of the senior leadership team] 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. Staff will not delete any material. 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. 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:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our searches and confiscation policy

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. 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 (via the app 'Securely' the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Acceptable use guidelines for the use of Artificial Intelligence

Pupils may use AI tools when:

- Approved by a teacher or staff member: Pupils must only use AI systems that have been reviewed and authorised by the school.
- Supervised at all times: Children must not interact with AI tools without adult supervision, even if the tool is designed for education.
- Used for learning: AI tools can be used to support learning goals (e.g., to read aloud,

give feedback on spelling, help translate words for EAL pupils).

- Integrated into structured lessons: Teachers may include AI-based features in their lessons if they are age-appropriate and educational.
- Within clear limits: Pupils are taught that AI can be helpful but doesn't always provide correct answers or understand emotions.

Pupils will be taught:

- That AI is not a human and cannot replace a teacher.
- That AI can sometimes make mistakes or show bias.
- To report anything unusual, confusing, or upsetting that they see when using AI tools.

Pupils must not:

- Attempt to "trick" or "jailbreak" AI (e.g., trying to get an AI tool to say something rude, violent, or inappropriate).
- Use AI tools without permission or supervision, including on personal devices at school.
- Use AI to generate or share content that is harmful, misleading, violent, discriminatory, or adult in nature.
- Share any personal data with AI platforms, including names, school details, locations, or photos.
- Copy and paste AI-generated answers into their work unless a teacher has said it is okay (e.g. for research or accessibility).
- Use AI to create fake news, deep fakes, impersonate others, or manipulate content.

All pupils will be reminded that misuse of AI will be treated as a breach of the school's behaviour policy and online safety rules.

Staff may use AI tools when:

- Used to support teaching and learning (e.g., planning lessons, generating ideas, or supporting pupils with SEND).
- Creating resources such as differentiated tasks, worksheets, or interactive quizzes—with human oversight.
- Helping pupils use AI tools that are appropriate and within a clearly defined educational purpose.
- Protecting pupil privacy by using anonymised data (e.g., generating feedback without sharing pupil names).
- Contributing to workload reduction through safe, reviewed, and ethical use of generative AI tools.
- The school retains full accountability for how AI tools are used—AI cannot be used to delegate responsibility.

Parents/carers are encouraged to:

- Discuss AI with their children at home in a positive, supportive, and age-appropriate way.
- Support school policies by ensuring AI is not misused at home (e.g., completing homework via AI without permission).
- Attend information sessions or read updates from the school about safe AI use.
- Contact the school with concerns about AI tools used in class or at home.

Parents must not:

- Encourage or permit their child to use AI for dishonest purposes (e.g., copying homework answers).
- Share or post AI-generated content (e.g., classwork or reports) online without school permission.
- Use AI to impersonate or create false communications.
- Enter their child's personal data into external AI tools without knowing how the data is stored or used.

Safeguarding and Privacy in regard to Artificial Intelligence

- All AI systems must be compliant with UK GDPR and relevant safeguarding legislation.
- No identifiable pupil data may be input into public or third-party AI systems without explicit parental consent.
- The school will not use AI for surveillance or monitoring pupils without justification and oversight.
- All staff must report AI-related safeguarding concerns or incidents to the **Designated Safeguarding Lead (DSL)** immediately.
- AI tools must not replace staff judgment in safeguarding decisions or pupil welfare.

When vetting an AI tool, staff must ask:

- Does this tool collect or store pupil data?
- Does it generate open-ended content?
- Could it produce harmful or inappropriate output?
- Has a Data Protection Impact Assessment (DPIA) been completed?

8. Pupils using mobile devices in School

Pupils in Y6 may bring mobile devices into school which are then handed in to a staff member for the duration of the school day.

Pupils are not permitted to bring in or use devices such as Smart watches, which have a camera, internet connectivity and/or mobile technology (can be used for messages and calls).

9. Staff using work devices outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

Our ICT Manager will ensure that anti-virus and anti-spyware software is installed and operating systems are up to date. Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our relational behaviour policy.
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. If such incidents involve illegal activity or content, they will be reported to the police.
Data Protection, GDPR, and AI

- To ensure compliance with the UK GDPR and the Data Protection Act 2018:
- All AI tools must be approved by the Data Protection Officer (DPO) or SLT before use.
- Personal pupil data may not be entered into AI systems.
- Any breaches need to be reported to Operations Managers and Data Protection Lead for the Trust asap.

11. 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. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, staff meetings and briefings. The DSL [and deputy DSL] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also 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. Volunteers will receive appropriate training and updates. More information about safeguarding training is set out in our child protection and safeguarding policy.

Training regarding Artificial Intelligence

Continuous Evaluation

- The effectiveness, risks, and appropriateness of AI tools must be regularly reviewed.
- Staff and leadership must remain informed about the evolving nature of AI and its implications for education, safety, and ethics.
- The school will adapt practices and policies in line with new research, guidance from government or education bodies, and technological developments.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety via coms and or via our 'Low Level Concern' log. This policy will be reviewed every year by the Executive Headteacher. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Relational behaviour policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Whistleblowing policy and Low-Level Concern policy
- ICT and internet acceptable use policy

14.Appendices

Appendix 1	Acceptable use agreement (Staff, Governers, Volunteers and Visitors

Appendix 1 – Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
• I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. • I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. • I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. • I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
Signed (staff member/governor/volunteer/visitor): **Date:**