

Three Counties Academy Trust



Online Safety Policy

#SG43

Last amended 3rd September 2026 (v1.0)

Policy lifespan: 3 years. Subject to annual compliance check. Next full review 2nd September 2029.

Version history

Date	Version	Details	Actioned by	PDF to Websites	Word to Governor Hub
03.09.26	1.0	Formatted to house style and checked against model for updates. Ensured KCSIE 2026 compliance.	MF	✓	✓

Contents:

Version history

Policy abbreviations and acronyms

Statement of intent

Member, Trustee, Local Governor and Staff Summary

Parent Summary

1. Legal framework
2. Roles and responsibilities
3. Managing online safety
4. Cyberbullying
5. Child-on-Child sexual abuse and harassment
6. Grooming and exploitation
7. Mental health
8. Online hoaxes and harmful online challenges
9. Cyber-Crime

10. Online safety training for staff

11. Online safety and the curriculum

12. Use of technology in the classroom

13. Use of mobile devices

14. Educating parents

15. Internet access

16. Filtering and monitoring online activity

17. Network security

18. Emails

19. Artificial Intelligence (AI)

20. Social networking

21. TCAT school websites

22. Use of devices

23. Remote learning

Monitoring and review

Trust Glossary

Policy Abbreviations and Acronyms

AI	Artificial Intelligence
DBS	Disclosure and Barring Service
DfE	Department for Education
DSL	Designated Safeguarding Lead
ICT	Information Communication Technology
ID	Identification
KCSIE	Keeping Children Safe in Education
MAT	Multi-Academy Trust
SCR	Single Central Record
SLT	Senior Leadership Team
TCAT	Three Counties Academy Trust
UK GDPR	UK General Data Protection Regulation

NB. Where the term “parent” or “parents” is used this includes those who act as carers or have parental responsibility.

NB. Staff roles noted within this policy may also include those staff performing that role in an ‘Acting’ capacity.

Statement of intent

Three Counties Academy Trust (TCAT) recognises that technology and online services play a vital role in education, communication, learning, creativity and preparation for life in modern Britain. We are committed to ensuring that all pupils can benefit from the opportunities provided by digital technologies whilst being protected from harm.

TCAT believes that effective online safety is an essential component of safeguarding and child protection. Online risks are considered within our wider safeguarding arrangements, and we work proactively to create a culture where pupils, staff, Trustees, Local Governors, volunteers, parents and carers understand how to use technology safely, responsibly and respectfully. We are committed to educating and empowering children to make informed decisions online, develop digital resilience and seek support whenever concerns arise.

We recognise that safeguarding incidents can occur both online and offline and that children may be at risk from individuals they know, as well as from those they have never met. We also acknowledge the rapidly changing nature of technology, including social media platforms, online gaming, livestreaming services, messaging applications and emerging technologies such as artificial intelligence (AI), which can present both educational opportunities and safeguarding risks.

TCAT adopts a whole-trust approach to online safety that encompasses effective filtering and monitoring systems, robust policies and procedures, curriculum provision, staff training, education for parents and carers, and clear reporting mechanisms. Online safety considerations are embedded throughout teaching, learning, safeguarding and governance arrangements.

The breadth of issues within online safety is considerable; however, risks can broadly be categorised into four areas:

Content

Being exposed to illegal, inappropriate, harmful or misleading content, including pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, serious violence, misinformation, disinformation, conspiracy theories and content that promotes harmful behaviours

Contact

Being subjected to harmful online interaction with others, including peer-on-peer abuse, bullying, coercion, exploitation, commercial pressures, adults posing as children, grooming, criminal exploitation, sexual exploitation, financial exploitation and harmful interactions with AI-enabled or AI-generated services

Conduct

Behaviour online that causes or increases the risk of harm, including online bullying, harassment, sharing or creating harmful content, the sending, receiving or requesting of nude or semi-nude images, inappropriate use of AI technologies, and behaviours that adversely affect the wellbeing, safety or reputation of individuals

Commerce

Risks associated with online financial activity, including phishing, scams, fraud, inappropriate advertising, gambling, financial exploitation, identity theft and the misuse of personal information

Through this policy and related safeguarding procedures, TCAT seeks to ensure the safe, appropriate and responsible use of the internet, digital technologies and online services by all members of the trust community. We are committed to maintaining an environment in which children are safeguarded, supported and educated to navigate the online world safely and confidently, whilst enabling staff to use technology effectively in support of teaching, learning and operational excellence.

Member, Trustee, Local Governor and Staff Summary

Purpose

- Online safety is an integral part of safeguarding and child protection
- The policy protects pupils from online risks whilst enabling safe and beneficial use of technology
- TCAT adopts a whole trust approach including education, training, filtering, monitoring and reporting systems

Key Safeguarding Risks

- Addresses content, contact, conduct and commerce risks
- Covers cyberbullying, grooming, exploitation, radicalisation, harmful online challenges and cybercrime
- Recognises emerging risks associated with artificial intelligence (AI)

Leadership and Governance

- The Trust Board and Local Governing Bodies ensure statutory compliance and oversight of online safety arrangements
- DSLs lead online safety within schools and monitor incidents, trends and safeguarding concerns
- An Online Safety Coordinator supports education, training, awareness and information sharing across TCAT

Education and Training

- Online safety is embedded across the curriculum and reinforced through assemblies and wider safeguarding activity
- Staff receive regular safeguarding and online safety training, including emerging risks and filtering and monitoring responsibilities
- Parents are supported through newsletters, training events, resources and regular updates

Filtering and Monitoring

- Appropriate filtering and monitoring systems are implemented and reviewed regularly
- Roles and responsibilities are clearly assigned to ensure effective oversight and response
- Concerns identified through monitoring are managed through safeguarding procedures

Responding to Concerns

- All online safety incidents, disclosures and concerns are reported and managed through safeguarding processes
- Concerns involving child-on-child abuse, sexual harassment, exploitation or radicalisation are escalated appropriately
- Accurate records are maintained and trends are reviewed to strengthen practice

Artificial Intelligence

- Pupils are taught to use AI safely, responsibly and appropriately
- Systems are in place to reduce access to harmful AI-generated content
- Staff must use AI in accordance with trust policies and data protection requirements

Parent Summary

Our Commitment

- Keeping children safe online is a key part of safeguarding and child protection
- Pupils are taught to use technology safely, responsibly and respectfully
- Online safety is supported through education, filtering, monitoring and reporting systems

Online Risks

- Children are taught about harmful content, unsafe contact, risky online behaviour and online scams
- The curriculum covers cyberbullying, grooming, exploitation, radicalisation and AI-related risks
- Pupils learn when and how to seek help if something concerns them online

How We Keep Children Safe

- Appropriate filtering and monitoring systems help reduce exposure to harmful content
- Online safety is taught through the curriculum, assemblies and safeguarding activities
- Concerns are managed by safeguarding staff and recorded appropriately

Mobile Devices and Social Media

- Personal mobile devices are not normally permitted for pupil use during the school day
- Misuse of technology, including bullying or sharing harmful content, is addressed promptly
- Pupils are encouraged to use technology responsibly both in and out of school

Artificial Intelligence (AI)

- Pupils are taught to use AI safely and appropriately
- Our schools take steps to prevent access to harmful AI-generated content
- Children are supported to recognise misinformation, manipulation and online deception

Working With Parents

- Parents receive advice, updates and resources about online safety risks
- Guidance is provided on parental controls, online behaviour and emerging technologies
- Online safety information is shared through newsletters, events and Wake Up Wednesday communications

What Parents Can Do

- Talk regularly with your child about their online experiences
- Use parental controls and privacy settings where appropriate
- Report concerns to the school if you believe a child may be at risk online

1. Legal framework

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

- [Online Safety Act 2023](#)
- [Voyeurism \(Offences\) Act 2019](#)
- [The UK General Data Protection Regulation \(UK GDPR\)](#)
- [Data Protection Act 2018](#)
- [Data \(Use and Access\) Act 2025](#)
- [Children's wellbeing and schools Act 2026](#)
- [DfE 'Filtering and monitoring standards for schools and colleges'](#)
- [DfE 'Harmful online challenges and online hoaxes'](#)
- [DfE 'Keeping children safe in education'](#)
- [DfE 'Teaching online safety in schools'](#)
- [DfE 'Searching, screening and confiscation'](#)
- [DfE 'Generative artificial intelligence \(AI\) in education'](#)
- [Department for Digital, Culture, Media and Sport and UK Council for Internet Safety 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'](#)
- [UK Council for Child Internet Safety 'Education for a Connected World – 2020 edition'](#)
- [National Cyber Security Centre 'Small Business Guide: Cyber Security'](#)

Where legislation has been passed or updated during the shelf life of this policy, we will always apply the latest version available irrespective of the version quoted here.

This policy operates in conjunction with the following policies:

- Behaviour Policy
- Cyber Crash Files
- Cyber Response and Recovery Plan

- Remote Learning Policy
- Safe Use of AI Policy (CU14)
- Cyber-Security Policy (FI15)
- Staff ICT and Electronic Devices Policy (FI16)
- School Website Policy (FI17)
- Data Protection Policy (FI20)
- Disciplinary Policy and Procedure (HR3)
- Staff Code of Conduct (HR26)
- Staff and Volunteer Confidentiality Policy (HR32)
- Child Protection and Safeguarding Policy and Procedure (SG1)
- Prevent Duty Policy (SG2)
- Allegations of Abuse Against Staff Policy (SG5)
- Photography and Images Policy (SG9)
- Child-on-Child Abuse Policy (SG10)
- Anti-Bullying Policy (SG19)
- Social Media Policy (SG24)
- Sharing Nudes and Semi-Nudes Policy (SG44)
- Mobile Devices Policy (SG45)

Central TCAT policies have the policy number identified, e.g. "SG1". Where no policy number is identified this indicates the policy is a school specific policy available from an individual TCAT school's website.

2. Roles and responsibilities

The Trust Board and where delegated, Local Governing Bodies will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance
- Ensuring each DSL's remit covers online safety
- Reviewing this policy in line with the policy lifespan and annual review requirements

- Ensuring their own knowledge of online safety issues is up to date
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals
- Ensuring that there are appropriate filtering and monitoring systems in place across TCAT and our schools
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with the CFO, Senior ICT Technician and service providers
- Ensuring that school SLTs and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified
- Ensuring that all relevant TCAT and school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding

The CEO will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout TCAT's policies and procedures
- Ensuring online safety practices are audited and evaluated
- Working with school leadership and the Trust Board to update this policy
- Identifying and assigning roles and responsibilities to manage TCAT's filtering and monitoring systems
- Appointing an Online Safety Coordinator for TCAT

Executive Headteachers, Headteachers and Heads of School will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout their school's policies and procedures, including in those related to the curriculum
- Supporting their DSL and deputy DSLs by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety
- Ensuring their staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training
- Ensuring online safety practices are audited and evaluated within their schools

- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe, including promoting material disseminated to them by TCAT's Online Safety Coordinator
- Working with the DSL and Senior ICT Technician to conduct light-touch reviews of the effectiveness of this policy

DSLs will be responsible for:

- Taking the lead responsibility for online safety in their school
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO, TCAT's Online Safety Coordinator and the Senior ICT Technician
- Ensuring online safety is recognised as part of their school's safeguarding responsibilities and that a coordinated approach is implemented
- Ensuring safeguarding is considered in their school's approach to remote learning
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of their school community understand this procedure
- Understanding the filtering and monitoring processes in place at their school and ensuring they continue to meet the school's safeguarding needs
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at their school
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns
- Monitoring online safety incidents to identify trends and any gaps in their school's provision and using this data to update the school's procedures
- Reporting to the Local Governing Body about online safety at each meeting, in person or as part of the Headteacher or Head of School's Report
- Working with their Executive Headteacher and Head of School, or their Headteacher and the Senior ICT Technician to conduct regular light-touch reviews of this policy in action

TCAT's Online Safety Coordinator will be responsible for:

- Contribute to each school's online safety education programme
- Raise awareness of online safety risks amongst pupils, staff and parents
- Coordinate online safety training, information and resources
- Facilitate the sharing of online safety information and safeguarding alerts
- Support DSLs in managing online safety incidents and concerns
- Review emerging risks and recommend improvements to policy and practice

The Senior ICT Technician will be responsible for:

- Providing technical support in the development and implementation of TCAT's online safety policies and procedures
- Implementing appropriate security measures as directed by the CFO, Executive Headteachers and Headteachers
- Ensuring that TCAT's and each school's filtering and monitoring systems are updated as appropriate
- Working with school leaders and DSLs to conduct regular light-touch reviews of this policy in action

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to
- Modelling good online behaviours
- Maintaining a professional level of conduct in their personal use of technology
- Having an awareness of current and emerging online safety issues
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online
- Reporting concerns in line with TCAT's and their school's reporting procedures
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum

Pupils will be responsible for:

- Adhering to all school ICT rules and other relevant policies.

- Seeking help from school staff if they are concerned about something they or a peer have experienced online
- Reporting online safety incidents and concerns in line with the procedures within this policy

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people. Staff will understand that pupils are at risk of abuse and other safeguarding concerns online as well as face to face, and in many cases, abuse will take place concurrently online and offline.

DSLs have overall responsibility for their school's approach to online safety, with support from deputies and their Headteacher/Head of School where appropriate and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. DSLs should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all TCAT and our schools operations in the following ways:

- Staff, Trustees and Local Governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted on the topic of remaining safe online
- Parents receive regular updates via letter, newsletters and the Wake-Up Wednesday communications
- Parents are invited to attend an annual information event for online safety

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with TCAT's Child Protection and Safeguarding Policy and Procedure.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the Executive Headteacher, Headteacher or Head of School, who decides on the best course of action in line with the relevant policies. If the concern is about the Executive Headteacher, Headteacher or Head of School, or a member of TCAT's Central Team, it is reported to the CEO. If the concern is about the CEO, it is reported to the Chair of the Trust Board.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher/Head of School and the Senior ICT Technician and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and TCAT's Child Protection and Safeguarding Policy and Procedure.

Where there is a concern that illegal activity has taken place, the Executive Headteacher, Headteacher or Head of School contacts the police.

The school will avoid unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. where a pupil has shared nudes or semi-nudes of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy and Procedure.

All online safety incidents and the school's response will be recorded by the DSL.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages

- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry

Our schools will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as lesbian, gay, bisexual, or gender questioning pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with TCAT's Anti-Bullying Policy.

5. Child-on-Child sexual abuse and harassment

Pupils may use the internet and technology to facilitate child-on-child sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, offline and online, and that online elements may facilitate or accompany abuse that also occurs face to face.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual making or sharing of nudes and semi-nudes, including those generated or altered using AI.
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing nudes or semi-nudes involving other children, including images generated or altered using AI may constitute a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves. Such incidents will be handled in accordance with TCAT's Sharing of Nude and Semi-Nudes Policy.

Our schools will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with TCAT's Child-on-Child Abuse Policy, Child Protection and Safeguarding Policy and Procedure, and the Social Media Policy.

Our schools will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using TCAT-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with TCAT's Child-on-Child Abuse Policy and the Child Protection and Safeguarding Policy and Procedure.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. DSLs will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online

- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways online. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production or distribution of child sexual abuse material (CSAM), or the sexual exploitation and trafficking of children.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting (including county lines activity), shoplifting, serious violence and other forms of criminal exploitation. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating online.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to their DSL without delay, who will manage the situation in line with TCAT's Child Protection and Safeguarding Policy and Procedure.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in TCAT's Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to their DSL without delay, who will handle the situation in line with TCAT's Child Protection and Safeguarding Policy and Procedure and Prevent Duty Policy.

7. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. DSLs will ensure that training is available to help ensure that staff members understand apps, games and websites, online terminology, the ways in which social interactions online in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with TCAT's Social, Emotional and Mental Health (SEMH) Policy.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online, e.g. via social media, game chats, and messaging platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video online, e.g. through social media channels, and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff become aware of, or suspect, a harmful online challenge or online hoax that may pose a risk to pupils, they will report this to their DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher/Head of School will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes
- Careful to avoid needlessly scaring or distressing pupils
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils
- Proportional to the actual or perceived risk
- Helpful to the pupils who are, or are perceived to be, at risk
- Appropriate for the relevant pupils' age and developmental stage
- Supportive
- In line with TCAT's Child Protection and Safeguarding Policy and Procedure

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

The DSL and Headteacher/Head of School will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

9. Cyber-Crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable

TCAT schools will factor into their approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher/Head of School will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

DSLs will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum taught across TCAT schools; however, it is particularly addressed in the following subjects:

- RSHE (secondary provisions)
- Relationships and health education (primary provisions)
- PSHE
- Citizenship
- ICT

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum.

TCAT schools approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content risks

Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as AI-generated content, deepfakes, pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact risks

Our schools will educate pupils about the potential dangers of interacting with others online or generative AI applications that simulate this. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct risks

Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with making, sharing or receiving nudes and semi-nudes, including images that have been generated or altered using AI. Online bullying, including the use online platforms, e.g. social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce risks

The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

DSLs will be involved with the development of their school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. SENCOs and designated teachers for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

Our schools will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. Executive Headteachers/Headteachers in consultation with their DSLs will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to

best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy and Procedure.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy and Procedure.

12. Use of technology in the classroom

A wide range of technology will be used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras
- Interactive whiteboards and touchscreen displays
- TCAT issued mobile phones used by staff for school purposes
- Video conferencing platforms
- Virtual learning environments (VLEs)
- Cloud-based learning and collaboration platforms
- Educational apps and software
- Web-based learning resources and websites
- Digital assessment and testing platforms

- Artificial intelligence (AI) tools and applications
- Printers, scanners and multifunction devices
- Audio recording devices
- School websites
- Social media accounts operated by the school
- Online storage and file-sharing platforms
- Messaging and communication platforms used for educational purposes
- Streaming and media-sharing platforms
- Online research databases and digital libraries
- Educational gaming and simulation platforms
- Translation devices

Prior to using any websites, tools, apps, AI systems or other online platforms in the classroom, or recommending that pupils use these platforms at home, the teacher will review and evaluate the resource to ensure it is appropriate, safe and suitable for the age and needs of the pupils. Teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be supervised when using online materials during lesson time – this supervision will be suitable to their age and ability.

13. Use of mobile devices

While TCAT recognises that the use of mobile devices can have educational benefits, there are also a variety of associated risks which our schools will ensure they manage.

Pupils will not be permitted to use personal mobile devices at any point during the school day unless exceptions apply. The prohibited use of personal mobile devices will be managed in accordance with TCAT's Mobile Devices Policy and any agreed exemptions in place.

Staff will use all personal technology in line with TCAT's Staff ICT and Electronic Devices Policy.

TCAT recognises that pupils may have access to the internet through personal devices and mobile phone networks outside the school day, or where school restrictions are circumvented. This can increase the risk of online behaviour that places pupils at risk of harm and breaches the TCAT's Mobile Devices Policy.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with their Behaviour Policy.

Inappropriate use of smart technology may include:

- Using mobile devices to sexually harass, bully, troll or intimidate peers
- Making or sharing nudes and semi-nudes, including images generated or altered using AI, both consensually and non-consensually
- Viewing and sharing pornography and other harmful content

TCAT schools will hold age-appropriate assemblies, where appropriate, which address any specific concerns related to the misuse of technology and outline the importance of using technology in an appropriate manner.

Our schools will seek to ensure that they remain up to date with emerging technologies, including AI tools, devices, platforms, apps, trends and related risks.

Our schools will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

14. Educating parents

TCAT and our schools will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about TCAT's approach to online safety and their role in protecting their children.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming
- Exposure to radicalising content

- Making or sharing nudes and semi-nudes, including images generated or altered using AI
- Cyberbullying
- Exposure to age-inappropriate content, e.g. pornography
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters
- Online resources
- Publication of Wake-Up Wednesday communications

15. Internet access

Pupils, staff and other members of the TCAT community will only be granted access to their school's internet network.

All members of the TCAT community will be encouraged to use their school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and monitoring online activity

The Trust Board will ensure TCAT's, and our schools ICT networks have appropriate filters and monitoring systems in place and that it is meeting the DfE's [Filtering and monitoring standards for schools and colleges](#). The Trust Board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

TCAT and our schools will do all we reasonably can to limit pupils' exposure to online risks from our ICT systems. TCAT will put in place appropriate filtering and monitoring systems and ensure that their effectiveness is reviewed at least annually and whenever there is a significant change to our networks, safeguarding risks or technology provision. Reviews will be carried out by the CFO and Senior ICT Technician.

Reviews will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record will be kept of these checks.

DSLs will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet their school's safeguarding needs.

The CFO, in collaboration with the Senior ICT Technician, Executive Headteachers, Headteachers and Heads of School will undertake a risk assessment to determine what filtering and monitoring systems are required within each TCAT school. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

Requests regarding making changes to the filtering system will be directed to the CFO and Senior ICT Technician. Prior to making any changes to the filtering system, the CFO and the Senior ICT Technician will conduct a risk assessment. Any changes made to the system will be recorded by the Senior ICT Technician. Reports of inappropriate websites or materials will be made to the Senior ICT Technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the appropriate DSL and Senior ICT Technician, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the school's Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with TCAT's Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

TCAT's networks and TCAT-owned devices will be appropriately monitored. All users of our networks and TCAT-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy and Procedure.

17. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by the Senior ICT Technician. Firewalls will be switched on at all times. The Senior ICT Technician will review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to ICT technicians.

All members of staff will have their own unique usernames and private passwords to access TCAT's systems. Where appropriate to do so, pupils will be provided with their own unique username and private passwords. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire at regular intervals, after which users will be required to change them.

Users will inform the Senior ICT Technician if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, their Headteacher/Head of School will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

The CFO and Senior ICT Technician will be responsible for implementing appropriate network security measures in liaison with TCAT's service providers, the DPO and DSLs. Full details of TCAT's network security measures can be found in the Cyber-Security Policy.

18. Emails

Access to and the use of emails will be managed in line with TCAT's Data Protection Policy, and the Pupil Confidentiality Policy, and Staff and Volunteer Confidentiality Policy.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Personal email accounts will not be permitted to be used on any TCAT site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail and report the email to the Senior ICT Technician. TCAT's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. The TCAT Central Team will organise annual cyber awareness training, including guidance on recognising phishing emails, AI-generated phishing attempts and other malicious communications. This training will include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking “does the email urge you to act immediately?”
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan and school specific Cyber Crash Plans.

19. Artificial Intelligence (AI)

TCAT and our schools will take steps to prepare pupils for changing and emerging technologies, including generative AI, and teach them how to use AI safely, responsibly and appropriately, taking account of their age and developmental stage.

TCAT will ensure its ICT systems include appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

Our schools will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

TCAT and our schools will take steps to ensure that personal, confidential or sensitive information is not entered into AI tools unless this is authorised, secure and compliant with data protection legislation.

Where staff use AI tools to support teaching, learning or administrative tasks, they will do so in accordance with the TCAT's Safe Use of AI Policy and DfE guidance on generative AI in education.

TCAT and our schools will make use of any guidance and support that enables them to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

20. Social networking

The use of social media by staff and pupils will be managed in line with TCAT's Social Media Policy.

21. TCAT school websites

Executive Headteachers, in collaboration with their Heads of School or Headteachers, will be responsible for the overall content of their school websites – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

All TCAT related websites will be managed in line with TCAT's School Website Policy.

22. Use of devices

Staff members and pupils will be issued with TCAT-owned devices to assist with their work, where necessary. The use of personal devices on TCAT premises and for the purposes of school work will be managed in line with the Staff ICT and Electronic Devices Policy.

23. Remote learning

All remote learning will be delivered in line with that school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

Monitoring and review

Lifespan of Policy: 3 Years

At any point this policy is updated or fully reviewed, it will be updated on the main TCAT website and will automatically update on all TCAT school websites simultaneously.

Where an annual check or other check results in minor changes, the Version History will be reviewed and updated with a change in the number following the decimal point, for example, v1.1 ⇒ v1.2. Where the policy is reviewed in full, then the number before the decimal point will change and reset, for example v1.4 ⇒ v2.0.

Any changes made by the CEO in collaboration with the Board Appointed Trustee will be passed to the Trust Board for ratification and subsequently be notified to Clerks to Local Governing Bodies and Headteachers/Heads of School.

The next scheduled full review date for this policy is 2nd September 2029.

Date approved by the Board Appointed Trustee: 3rd September 2026.

To be ratified and recorded in the minutes at the first Trust Board Meeting after 3rd September 2026.

Trust Glossary

AA	Admissions Authority	H&S	Health and Safety
AAI	Adrenaline Auto-Injector (Epi Pen)	HoS	Head of School
ACM	Asbestos Containing Materials	HSE	Health and Safety Executive
AHT	Assistant Headteacher	ICO	Information Commissioners Office
AIR	Attendance Intervention Reviews	IDSR	Inspection Data Summary Report
APDR	Assess Plan Do Review Cycle	IHP	Individual Healthcare Plan
APIs	Application Programming Interfaces	IRMS	Information and Records Management Society
ASC	Autistic Spectrum Condition	IWF	Internet Watch Foundation
ASP	Analyse School Performance	KCSIE	Keeping Children Safe in Education
ATH	Academy Trust Handbook	KS1/2/3/4	Key Stage 1/2/3/4
BAME	Black, Asian and Minority Ethnic Backgrounds	LAC	Looked After Child
BAT	Board Appointed Trustee	LADO	Local Authority Designated Officer
BCP	Business Continuity Plan	LGB	Local Governing Body
BFR	Budget Forecast Return	LLC	Low-Level Concerns
CEO	Chief Executive Officer	LSA	Learning Support Assistants
CFO	Chief Financial Officer	MASH	Multi-Agency Safeguarding Hub
CIF	Condition Improvement Fund	MAT	Multi-Academy Trust

CIN	Child in Need	MFA	Multi-Factor Authentication
CLA	Children Looked After	MFL	Modern Foreign Language
CMIE	Child Missing in Education	NCSC	National Cyber Security Centre
COO	Chief Operating Officer	NoV	Note of Visit
COSHH	Control of Substances Hazardous to Health	NPQ	National Professional Qualifications
CP	Child Protection	PA	Persistent Absence
CPD	Continuing Professional Development	PAN	Published Admission Number
CPOMS	Child Protection Online Management System	PECR	Privacy and Electronic Communications Regulations
CSCS	Children's Social Care Services	PEP	Personal Education Plan
CSE	Child Sexual Exploitation	PEEP	Personal Emergency Evacuation Plan
CTIRU	Counter-Terrorism Internet Referral Unit	PEx	Permanent Exclusion
CWD	Children with Disabilities	PP	Pupil Premium
CYPMHS	Children and Young People's Mental Health Services	PPG	Pupil Premium Grant
DBS	Disclosure and Barring Service	PSHE	Personal, Social and Health Education
DDSL	Deputy Designated Safeguarding Lead	PSED	Public Sector Equality Duty
DfE	Department for Education	PTFA	Parent, Teacher and Friends Association
DHT	Deputy Headteacher	QA	Quality Assurance

DSE	Display Screen Equipment	RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations
DSL	Designated Safeguarding Lead	RHE	Relationships and Health Education
DPO	Data Protection Officer	RPA	Risk Protection Arrangement
EAL	English as an Additional Language	RSHE	Relationships, Sex and Health Education
ECT	Early Career Teacher	SA	Severely Absent
EDIB	Equality, Diversity, Inclusion and Belonging	SALT	Speech and Language Therapist
EHA	Early Help Assessment	SARC	Sexual Assault Referral Centre
EHENA	Education, Health and Care Needs Assessment	SBM	School Business Manager
EHCP	Education, Health and Care Plan	SCC	Standard Contractual Clause
EHE	Elective Home Education	SCITT	School-Centred Initial Teacher Training
ELSA	Emotional Literacy Support Assistant	SCR	Single Central Record
ESFA	Education and Skills Funding Agency	SDP	School Development Plan
EVC	Educational Visit Coordinator	SDQ	Strengths and Difficulties Questionnaire
EWOSSE	Education Welfare and Safeguarding Support Officer	SEF	Self-Evaluation Form
EYFS	Early Years Foundation Stage	SEMH	Social, Emotional, and Mental Health
FBV	Fundamental British Values	SENCO	Special Educational Needs Coordinator
FFT	Fischer Family Trust	SEND	Special Educational Needs and Disabilities

FGM	Female Genital Mutilation	SIP	School Improvement Partner
FGMPO	FGM Protection Order	SLA	Service Level Agreement
FOI	Freedom of Information	SLCN	Speech, Language and Communication Needs
FSM	Free School Meals	SLT	Senior Leadership Team
FTS	Find a Tender Service	SPOC	Single Point of Contact
GAG	General Annual Grant	STEM	Science, Technology, Engineering and Maths
GDPR	General Data Protection Regulation	TA	Teaching Assistant
GIAS	Get Information about Schools	TAC	Team Around the Child
HASH	Herefordshire Association of Secondary Heads	TCAT	Three Counties Academy Trust
HBA	Honour Based Abuse	TUPE	Transfer of Undertakings (Protection of Employment)
HR	Human Resources	VSH	Virtual School Headteacher