Trust Education Group Ltd

Online Safety Policy

Statement of Intent

Trust Education recognises that the effective use of online services is essential for raising educational standards, supporting student achievement, and enhancing both teaching and learning. Digital technologies and online platforms are embedded in the daily life of our school community. Consequently, a robust framework of controls is in place to safeguard all students and staff.

Online safety is a complex and evolving area, with risks broadly grouped into four key categories:

Content: Exposure to illegal, inappropriate, or harmful material, including but not limited to pornography, misinformation, content promoting self-harm or suicide, and discriminatory or extremist views.

Contact: Dangerous interactions online, such as peer pressure, targeted advertising, or predatory behaviour by adults posing as children or young people for grooming or exploitation.

Conduct: Risky personal behaviour online, such as sharing explicit content, participating in cyberbullying, or engaging in harmful digital interactions.

Commerce: Dangers related to online gambling, misleading advertisements, phishing schemes, and other financial scams.

All safety protocols and protective measures at Trust Education are designed to address and mitigate these core risks. This policy sets out clear expectations to ensure that all students and staff engage with the internet and digital technologies in a safe, responsible, and respectful manner.

Legal Framework

This policy reflects full compliance with all relevant legislation and guidance, including, but not limited to:

- Voyeurism (Offences) Act 2019

Overview of the Act

The Voyeurism (Offences) Act 2019 was enacted to address specific acts of voyeurism that were not adequately covered by existing laws. It amends the Sexual Offences Act 2003 by introducing two new offences under section 67A, which criminalize the act of operating equipment or recording images

beneath another person's clothing without their consent, with the intent to observe their genitals or buttocks, whether covered or uncovered.

The UK General Data Protection Regulation (UK GDPR)

Overview of UK GDPR

The UK GDPR took effect on January 1, 2021, following the UK's exit from the EU. It is based on the EU GDPR but has been adapted to fit the UK legal context. The UK GDPR works alongside the Data Protection Act 2018 (DPA 2018), which provides additional details and exemptions related to data protection.

Data Protection Act 2025

Key Developments

Data (Use and Access) Bill: This bill is currently progressing through Parliament and is anticipated to receive Royal Assent in 2025. It proposes amendments to the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, focusing on enhancing data subject rights and streamlining data processing activities.

Changes to Data Subject Rights: The bill aims to clarify and potentially relax certain constraints related to automated decision-making and data processing for legitimate interests, which may impact how organizations handle personal data.

Regulatory Changes: The bill proposes to abolish the role of the Information Commissioner and transfer its functions to a new Information Commission, which could alter the enforcement landscape for data protection in the UK.

Impact on Businesses: Organizations will need to reassess their data protection practices in light of these changes, particularly regarding compliance with new provisions related to cookie management and direct marketing practices.

EU Adequacy Decisions: The UK's data protection framework is under scrutiny, especially concerning its compatibility with EU laws. The adequacy decisions that allow for the free flow of data between the UK and EU are set to expire in June 2025, making the outcomes of the Data (Use and Access) Bill critical for maintaining these arrangements.

DfE (2021) 'Harmful online challenges and online hoaxes'

The Department for Education (DfE), in partnership with the UK Council for Internet Safety Education subgroup and the Samaritans, has issued guidance to support schools and colleges in responding to harmful online challenges and online hoaxes. These resources may also be valuable for other educational settings, including Trust Education. A hoax is defined as a deliberate fabrication intended to mislead others while appearing to be truthful. Online challenges typically involve individuals filming themselves performing a task sometimes risky or dangerous and sharing the video on social media platforms, thereby encouraging others to take part.

DfE (2023) 'Filtering and monitoring standards for schools and colleges'

In line with the statutory guidance outlined in Keeping Children Safe in Education, governing bodies and proprietors must ensure that appropriate filtering and monitoring systems are in place to protect all users within the school environment.

Filtering – A Preventative Measure

Filtering involves the use of technology to restrict access to illegal, inappropriate, or potentially harmful content online. This is achieved by identifying and blocking specific websites or types of web content including text, images, audio, and video that pose a risk to users. Effective filtering is proactive and aims to prevent exposure before it occurs.

Monitoring – A Responsive Measure

Monitoring refers to systems and processes that observe and record user activity on digital devices. This can take two forms:

Manual Monitoring: For example, teachers supervising students by viewing their screens during lessons.

Technical Monitoring: Software installed on devices to track user activity. These systems can generate alerts or reports when they detect behaviour or content that is illegal, inappropriate, or potentially harmful such as online bullying or attempts to access restricted material.

Unlike filtering, monitoring solutions do not block access. Instead, they serve as a reactive tool, helping staff respond to incidents and ensure ongoing student safety.

DfE (2025) 'Keeping children safe in education 2025'

Keeping Children Safe in Education (KCSIE) 2025 is statutory guidance issued by the Department for Education (DfE) that outlines the legal duties and responsibilities schools and colleges in England must follow to safeguard and promote the welfare of children and young people. The guidance sets out clear expectations for all staff, governing bodies, and proprietors regarding:

- *Identifying and responding to signs of abuse or neglect*
- *Safer recruitment practices*
- *Online safety measures, including filtering and monitoring*
- *Child-on-child abuse and sexual violence*
- *The role of designated safeguarding leads (DSLs)*
- *Partnership working with external safeguarding agencies*
  All education settings, including Trust Education, are legally required to have regard to this guidance when carrying out their duties to ensure the safety and well-being of all pupils.

DfE (2023) 'Teaching online safety in school'

Teaching Online Safety Through the Curriculum

This non-statutory guidance outlines how schools can ensure pupils understand how to stay safe and behave appropriately online, by embedding online safety within existing curriculum requirements.It is designed to support and enhance learning across several key subjects, including:

- *Relationships Education*
- *Relationships and Sex Education (RSE)*
- *Health Education*
- *Citizenship*
- *Computing*

There are no additional teaching requirements introduced by this guidance.

The guidance is intended for school leaders, teaching staff, and governing bodies, and applies to:

- *Local-authority-maintained schools*
- *Academies*
- *Free schools*

Independent schools and non-maintained special schools may also find this guidance beneficial, as they are similarly required to deliver Relationships Education, RSE, and Health Education.

DfE (2022) 'Searching, screening and confiscation'

The appropriate use of searching, screening, and confiscation powers is an important aspect of safeguarding. When applied correctly, these measures help protect the welfare of pupils and staff and reinforce a culture of safety and respect across the school. This guidance aims to clarify the legal powers available to headteachers and authorised staff, ensuring they have the knowledge and confidence to use these powers when necessary and in accordance with statutory expectations.

Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

Sharing of Nude and Semi-Nude Images (UKCIS, 2024)

According to the latest guidance from the UK Council for Internet Safety (UKCIS, 2024), the sharing of nude or semi-nude images, videos, or live streams by young people under the age of 18 is a significant online safety concern. This behaviour often referred to in informal terms by young people as "pics" and can occur across a variety of platforms, including:

- *Social media*
- *Messaging or chat apps*
- *Gaming platforms*
- *Online forums*
- *Direct device-to-device sharing (e.g. via Bluetooth or AirDrop)*

It is important to recognise that the motivations behind creating or sharing such content are not always sexually or criminally driven. In some cases, young people may not fully understand the implications of their actions, or may be influenced by peer pressure, curiosity, or a desire for validation.

UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

Education for a Connected World is a key resource for anyone working with children and young people. It provides a structured approach to teaching and learning that helps children develop the knowledge, skills, and values they need to engage with the digital world safely, responsibly, and confidently.

The framework focuses on eight core aspects of online life:

- *Self-Image and Identity*
- *Online Relationships*
- *Online Reputation*
- *Online Bullying*
- *Managing Online Information*
- *Health, Wellbeing, and Lifestyle*
- *Privacy and Security*
- *Copyright and Ownership*

Designed to support and enhance the delivery of online safety education, this framework helps schools foster empowerment, resilience, and positive cultural change.

National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

The National Cyber Security Centre (NCSC) published the Small Business Guide: Cyber Security in 2018 to provide practical, accessible advice for smaller organisations including schools, on how to protect themselves from common cyber threats.

The guide outlines five key areas of cyber security best practice:

- *Backing up data – Ensuring important information is regularly and securely backed up to protect against data loss.*
- *Protecting devices – Using passwords, encryption, and anti-malware to safeguard computers, tablets, and smartphones.*
- *Keeping software up to date – Regularly installing updates to fix security vulnerabilities in operating systems and applications. Controlling access – Restricting who has access to what data and systems to reduce the risk of internal threats or accidental damage. Avoiding phishing attacks – Recognising and defending against malicious emails and scams designed to steal personal or financial information.*

Roles and Responsibilities

• Trust Education Group Ltd is tasked with ensuring the effectiveness of this policy and its compliance with all relevant legislation and statutory guidance. The safeguarding governor maintains oversight that the Designated Safeguarding Lead's (DSL) remit encompasses online safety, and it reviews this policy annually. It keeps its knowledge of online safety issues current and ensures all staff receive safeguarding and child protection training, including elements specific to online safety, as part of their induction. (please see Staff induction pack)

Trust Education Group Governors and Directors guarantee the implementation of robust filtering and monitoring systems, review of the effectiveness with staff and providers at least annually, and verifies that the Senior Leadership Team (SLT) and relevant staff understand and can manage these provisions. Furthermore, the board of governors oversees that policies effectively plan for and address online challenges and hoaxes.

• Trust Education group integrates online safety as an ongoing and interconnected theme within all school policies and procedures, notably those linked to the curriculum, staff training, and safeguarding. Trust education Group support

their staff team by allocating sufficient time and resources for their online safety duties. They ensure all staff receive regular, updated, and relevant online safety training, and that best practices are consistently reviewed and evaluated. Engagement with parents/carers is organised to keep them informed of current online safety issues and the measures in place to protect pupils. Trust Education Group sends out regular Online Safety bulletins to staff, incorporate Online Safety discussions in briefings and in staff meetings. Head of school participates in regular reviews of this policy and collaborates with the board of governors to update it annually.

• The Designated Safeguarding Lead (DSL) assumes lead responsibility for online safety across the Trust Education Group Ltd. The DSL serves as the primary contact for all online safeguarding issues and commits to ongoing training to deepen their understanding of online safety risks, particularly for pupils with SEND. The DSL recognises online safety as integral to safeguarding, ensures it is embedded in remote learning practices, and makes referrals to external agencies as needed. The DSL works closely with police during investigations, stays abreast of new research, legislation and trends, and organises school participation in online safety events. Robust procedures for reporting and recording incidents are maintained, and recorded on CPOMS. The DSL ensures all training includes clarity on roles, expectations, and processes regarding filtering and monitoring. They monitor incidents to identify trends, and update procedures, reporting to the governing board at least annually, and participate in regular policy reviews.

By clearly defining these responsibilities, Trust Education Group Ltd underlines its commitment to a safe and secure digital environment for the entire school community.

To ensure the effectiveness of these measures, all staff members at Trust Education Group share clear responsibilities regarding online safety. Each staff member is expected to:

- Take responsibility for the security of ICT systems and electronic data they use or have access to.
- Model good online behaviours, demonstrating safe and respectful use of technology to set a positive example for pupils.
- Maintain a professional level of conduct in their personal use of technology, upholding the trust and reputation of the school community.
- Remain aware of current and emerging online safety issues, adapting practice where necessary to safeguard pupils effectively.
- Ensure familiarity with the indicators that suggest a pupil may be unsafe online, so that early intervention is possible.
- Report any concerns in accordance with the school's established reporting procedures (CPOMS) ensuring timely and appropriate responses to incidents.

- Where relevant to their role, embed online safety within their teaching of the curriculum, equipping pupils with the knowledge and skills they need to navigate the digital world safely.

Pupils themselves also play an important part in sustaining a safe online environment. They are responsible for:

- Seeking help from school staff if they are concerned about something they or a peer have experienced online, recognising that support is available.
- Reporting online safety incidents and concerns to a trusted adult whenever appropriate, so that action can be taken to protect themselves and others.
- Following the school rules for using the internet, as displayed in classrooms, and around the school, and understanding that these guidelines are in place for their safety and wellbeing.

Managing online safety requires recognition from ALL staff. Technology plays a central role in many safeguarding and wellbeing issues impacting young people today. The widespread use of social media and the internet among children increases both opportunities and risks. Therefore, all staff must remain vigilant to the evolving nature of online threats and the potential impact these may have on pupils' welfare.

In cases of potentially harmful online sexual behaviour, the DSL must liaise promptly with the police or children's social care services, drawing on external expertise and support to ensure the wellbeing and safety of pupils. By taking a proactive and collaborative approach, the DSL and the wider safeguarding team can respond swiftly and appropriately to emerging online risks.

In recognition of these evolving challenges, the school ensures that the importance of online safety is thoroughly integrated into all its operations. This commitment is reflected in several key practices:

- All staff and governors participate in comprehensive online safety training, both at induction and each year thereafter, to maintain heightened awareness of the latest risks and best practices.
- Staff are kept informed of emerging threats and any updates to online safety legislation or guidance through timely email notifications, briefings, staff meetings and staff bulletins, ensuring that everyone remains up to date and vigilant.
- Online safety forms a core strand of the school curriculum, with learning opportunities woven throughout subject areas to equip pupils with practical digital literacy and critical thinking skills.

- The school actively engages the wider community by providing regular assemblies and newsletters, focusing on current online risks and the collective responsibility to stay safe in the digital world.

These measures foster a culture of continuous learning and shared responsibility, empowering both staff and pupils to respond confidently to online challenges and risks.

Handling online safety concerns

A clear, accessible reporting pathway is established so that pupils know how and where to seek help, and staff understand their responsibilities for responding to concerns. Confidentiality is balanced with the necessity of safeguarding, ensuring information is shared appropriately with relevant safeguarding leads or external agencies, while maintaining the dignity and privacy of those involved. Staff are encouraged to build trusting relationships with pupils, creating a supportive environment in which children feel safe to raise sensitive issues related to their online lives. Regular discussions and reminders reinforce that any concern, no matter how small it may seem, should be reported and addressed promptly.

Any disclosures made by pupils to staff, whether about their own experiences or on behalf of another child regarding online abuse, harassment, or exploitation are handled rigorously in accordance with the school's Child Protection and Safeguarding Policy which can be found on Trust Educations website. Staff are reminded that some pupils may not feel ready or able to share their experiences of abuse due to feelings of embarrassment, humiliation, fear, or as a result of Special Educational Needs and Disabilities. As such, staff maintain a keen awareness that the absence of reports does not equate to the absence of harmful online behaviour.

It is recognised that harmful online sexual behaviour often occurs on a continuum. Early and appropriate intervention is therefore essential to prevent escalation and further abuse. Staff also acknowledge that children exhibiting concerning behaviours online may themselves be victims and must be provided with suitable support.

Should a victim express a desire for confidentiality, the Designated Safeguarding Lead (DSL) will carefully weigh the pupil's wishes against their duty to protect the individual and others. The DSL will consider whether sharing details could cause additional harm or whether it is necessary for safeguarding purposes. Ultimately, the safety and welfare of the pupil will guide any decision, and the DSL, along with other relevant staff, will meet with the victim's parents/carers to discuss both safeguarding measures and the progression of the report.

While every effort is made to respect confidentiality, it cannot be promised where there is a legal requirement or safeguarding imperative to share information, for example under the public task basis of UK GDPR, where it is in the public interest. If

it becomes necessary to refer a matter to children's social care or the police against a pupil's wishes, this action will be handled with utmost sensitivity, and continuous support will be provided to the victim throughout.

Concerns about the online behaviour of staff are reported directly to Head of school, who will take appropriate steps in line with the Staff Code of Conduct, which can be found on Trust Education website. if the concern involves Head of School, it is reported to the chair of governors. Concerns about a pupil's online behaviour are referred to the DSL, who works with Head of School, ICT technician (if appropriate), and other staff, managing each case in accordance with the school's Behaviour Policy and Child Protection and Safeguarding Policy. Where there are suspicions of illegal activity, the police are contacted.

The school is mindful to avoid unnecessarily criminalising pupils when behaviour results from ignorance or normal developmental curiosity, such as the creation or distribution of indecent images. The DSL determines when a supportive rather than punitive response is most appropriate, always in line with the Child Protection and Safeguarding Policy.

All online safety incidents, along with the school's response, are carefully recorded on CPOMS by the DSL to ensure oversight, accountability, and ongoing improvement of safeguarding practices.

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, making it appear as though the victim is responsible
- Threatening or bullying emails, potentially sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted on blogs, personal websites, and social networking sites, such as Facebook
- Abuse between young people in intimate relationships online, i.e., teenage relationship abuse
- Discriminatory bullying online, such as homophobia, racism, misogyny, or misandry

Trust Education recognises that certain pupils may be at greater risk of abuse or bullying online, particularly those with Special Educational Needs and Disabilities (SEND), who are considered especially vulnerable. Cyberbullying directed at pupils

or staff is not tolerated under any circumstances. All incidents, regardless of where they occur, are managed promptly and effectively in accordance with the school's Anti-bullying Policy, ensuring a swift resolution and continued safeguarding of the school community.

Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

examples of online harmful sexual behaviour

- 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 sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will maintain an uncompromising stance against sexually harassing or abusive behaviour, actively promoting a zero-tolerance policy. Any attempt to minimise, dismiss, or justify such actions as trivial or harmless will not be accepted, as staff understand that this approach is essential to preventing a culture where abuse becomes normalised and pupils feel discouraged from coming forward. Staff are also acutely aware that the creation, possession, or distribution of indecent images of children defined as any person under 18 years of age is a criminal offence. This remains the case even if the imagery is produced, possessed, or shared consensually by the child themselves or with their permission. Trust Education is committed to ensuring all staff adhere to this guidance to safeguard pupils and uphold the highest standards of protection.

The school recognises that, after an incident of online harmful sexual behaviour is reported, interactions between the victim and the alleged perpetrator(s) frequently persist on social media platforms. In these digital spaces, the situation can be exacerbated by other pupils taking sides, which often leads to further harassment and perpetuates the cycle of abuse. The school will respond to such incidents in strict accordance with its children protection and safeguarding Policy. Ensuring that every concern is addressed thoroughly and consistently.

All concerns regarding online child-on-child sexual abuse and harassment are taken seriously, regardless of whether the incident occurred on school premises or involved school-owned equipment. Any such concerns must be reported without delay to the Designated Safeguarding Lead (DSL), who will conduct a prompt and comprehensive investigation following the procedures outlined in the Child protection and safeguarding Policy. This approach ensures that the well-being of all pupils is prioritised and that a robust safeguarding culture is maintained throughout the school community.

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, including the following:

- The pupil may believe they are communicating with another child, when in fact they are engaging with an adult who has assumed a false identity for the specific purpose of earning the pupil's trust and facilitating abuse.
- The pupil might be reluctant to disclose that they have been speaking with someone they met online, worried about possible judgement, embarrassment, or a lack of understanding from both peers and adults.
- Pupils can be manipulated into feelings of dependency on the groomer, especially if the perpetrator has managed to isolate them from their usual support systems, such as friends and family.
- The secretiveness and attention involved in such communications might make the pupil feel 'special', a feeling that can be amplified if the person they are talking to claims to be older or more experienced.
- Through calculated manipulation, pupils may develop a strong emotional bond to their groomer, marked by feelings of loyalty, admiration, or even love, often mixed with confusion, distress, or fear.

Given that pupils are less likely to report incidents of grooming compared to other online offences, it is especially important for staff to recognise the indicators of this form of abuse. The Designated Safeguarding Lead (DSL) will ensure that all online safety training highlights online abuse, emphasises vigilance for the signs of grooming, and clearly outlines what these signs may look like. Indicators may include:

- Secretive behaviour regarding how or where they are spending their time, particularly online.
- The presence of an older boyfriend or girlfriend, typically someone not known to the school community or the pupil's close friends.
- Unexplained acquisition of money or new possessions, such as clothes or technological devices, that the pupil either cannot or will not account for.

Child sexual exploitation (CSE) and child criminal exploitation (CCE) present further safeguarding concerns, with both forms of abuse increasingly facilitated through online platforms. CSE may involve not only physical sexual abuse or violence but also significant online elements, such as sexual coercion, manipulation, or encouraging children to engage in sexually inappropriate behaviours via the internet. In some instances, a pupil might be groomed online and subsequently drawn into broader exploitation networks, for example, becoming involved in the production of child sexual abuse material, forced prostitution, or sexual trafficking.

Similarly, CCE involves children being forced or manipulated into illegal activity' such as transporting drugs, shoplifting, or engaging in serious violence for the benefit of perpetrators. While these activities may occur face-to-face, there is a growing trend of children being targeted and groomed online, where abusers can exert influence and control from a distance, often concealing their identity.

Given the covert nature of both CSE and CCE, recognising subtle warning signs is critical. These may include unexplained absences from school, sudden changes in behaviour, withdrawal from friends and family, or signs of fear and anxiety related to online activity. Staff who have any concerns relating to possible CSE or CCE must report these immediately to the Designated Safeguarding Lead (DSL), who will respond in accordance with the school's Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process may develop through direct recruitment, such as individuals in extremist groups actively identifying, targeting, and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda online. Children who are targeted for radicalisation are often groomed by extremists via digital platforms to the point where they come to believe that these individuals have their best interests at heart, increasing the likelihood that they will adopt similar radical beliefs.

Staff members must be mindful of the factors that can heighten certain pupils' vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Vigilance is essential for recognising pupils who may display indicators of radicalisation or who are in the process of being groomed to adopt extremist ideologies. Where there are concerns relating to radicalisation, staff are required to report these immediately to the Designated Safeguarding Lead (DSL), who will respond in accordance with the Prevent Duty Policy.

Mental Health

It is also important to acknowledge that the online environment can have far-reaching effects on pupils' mental health. Social media platforms and other internet-based interactions, while offering opportunities for connection and support, can also expose children and young people to risks that may adversely affect their emotional wellbeing.

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

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. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

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, most often intended to scaremonger or to distress individuals who encounter it, and typically propagated through social media platforms. These hoaxes can rapidly gain traction and have a significant emotional impact on young people, especially when they are widely shared or appear to come from trusted sources.

"Harmful online challenges" refers to social media trends which encourage young people to record themselves taking part in online challenges and to share these videos, often daring others to participate in turn. While many online challenges are harmless or intended to foster a sense of community, they become a safeguarding concern when the activity puts participants at risk of harm, either directly, due to the nature of the challenge, or indirectly, through the online distribution of the video. The specific risk posed may depend on the age and vulnerability of the pupil involved, as well as on the context in which the video is shared and how the pupil is depicted.

Where staff suspect the presence of a harmful online challenge or an online hoax circulating among pupils, they must report this to the DSL without delay. The DSL will conduct a case-by-case assessment to determine the scale and nature of the risk, considering whether it is localised within the school or the wider community, or if it is part of a broader trend affecting young people nationally. In cases where a hoax or challenge appears to be spreading mainly in the local area, the DSL will consult with the Local Authority (LA) to explore swift interventions that could prevent further dissemination.

Prior to determining a response, the DSL will ensure that any proposed action aligns with guidance from reliable sources, such as the UK Safer Internet Centre, and that the risk is fact-checked. Responses will be carefully calibrated to avoid unnecessarily alarming or distressing pupils, and care will be taken not to inadvertently introduce

pupils to risks they might not have otherwise encountered, especially among younger children who may be unaware of the trend. The school will strive for a proportionate, age-appropriate, and supportive approach, always in line with the Child Protection and Safeguarding Policy.

If the DSL's assessment finds that an online challenge places pupils at risk, for example, by encouraging age-inappropriate or dangerous activities the school will take direct action targeted at those most affected, such as specific year groups, classes, or even individual pupils, as necessary. School-wide interventions will only be implemented when the risk of increasing exposure is outweighed by the need for broader awareness, and in such cases, careful consideration will be given to minimising unnecessary alarm.

Cyber-crime

Cyber-crime refers to criminal activities committed using computers and/or the internet, and it is important for the school community to understand its two main categories. Cyber-enabled crimes are offences that could take place offline but are made easier or more widespread by online technology for instance, fraud, the buying and selling of illegal drugs, or sexual abuse and exploitation. Cyber-dependent crimes, on the other hand, are offences that exist only because of the internet or computer technology, such as the creation or distribution of malware, illegal hacking, or 'booting' (overwhelming a network or website with traffic to make it unavailable).

The school acknowledges the particular risk that pupils with a keen interest or aptitude in technology may, intentionally or otherwise, become involved in cyber-crime. Where there are concerns about a pupil's engagement with technology and their intentions, the DSL will consider making a referral to the Cyber Choices programme, which seeks to redirect young people at risk of committing cyber-crime towards using their skills constructively and lawfully.

To prevent such issues and foster digital responsibility, the DSL and headteacher will ensure pupils are taught, throughout the curriculum, to use technology safely, responsibly, and legally. The school will also take active measures, such as appropriate firewalls and content filters, to prevent access to parts of the internet that may encourage unlawful activity, including the 'dark web', on any school-owned devices or networks.

To further strengthen the school's approach to online safety, all staff will receive safeguarding training that specifically includes elements of digital risk and protection. Designated Safeguarding Leads (DSLs) are responsible for ensuring that this training covers how the internet can be used as a medium for abuse and exploitation, equipping staff to recognise the signs and understand the ways technology can facilitate various forms of harm. The training will also clarify the expectations, roles, and responsibilities of staff regarding the school's filtering and

monitoring systems, ensuring that all members of the school community know how to use these protective measures effectively.

Staff will be made fully aware that pupils face risks of abuse both online and in person, and that abuse can often occur in parallel across digital and physical environments. By supporting staff to identify and respond to online threats whether perpetrated by peers or adults, the school reinforces its commitment to safeguarding pupils in all aspects of their lives.

Online Safety and the Curriculum

Online safety is not treated as a standalone concept but is thoroughly embedded across the curriculum, with particular emphasis in Relationship and Sex Education (RSE), Personal, Social, Health and Economic (PSHE) education, and ICT lessons. Teaching about online safety is always tailored to be age-appropriate and suitable for each pupil's developmental stage, ensuring that all learners gain the foundational knowledge and behaviours needed to navigate the online world safely and confidently, regardless of the device, platform, or app they may use.

Throughout the curriculum, pupils are taught to critically evaluate online content, recognise techniques used for persuasion, and understand what healthy, respectful relationships, including friendships look like in a digital context. Lessons and assemblies also address body confidence, self-esteem, consent, and the distinction between acceptable and unacceptable online behaviours. Pupils learn how to identify online risks, the importance of seeking support when needed, and how to discern when something is deliberately deceitful, harmful, or age-inappropriate. These core concepts are adapted to be developmentally appropriate for each age group, ensuring that learning is relevant and accessible.

Where appropriate, pupils themselves are consulted, recognising their unique insights into the types of websites they and their peers use and the digital behaviours they commonly engage in. The school acknowledges that while all pupils can be vulnerable to online harm, certain groups such as those with Special Educational Needs and Disabilities (SEND) or Looked After Children (LAC) may be more susceptible. Staff work collaboratively to tailor the curriculum, ensuring these pupils receive the targeted information and support they need.

A personalised or contextualised approach is adopted for children who are more at risk, or in response to incidents of harmful online behaviour within the school community. All external resources considered for use in teaching online safety are carefully reviewed by teachers, to ensure they are evidence-based, quality-assured, and suitable for the pupils' age and developmental stage. If external visitors are

invited to deliver aspects of the online safety curriculum, Head of school will ensure these visitors are appropriate and relevant to the needs of the pupils.

Before lessons or activities on online safety, the class teacher and DSL review the content and consider the possibility that some pupils in the class may have experienced, or be experiencing, online harm. The DSL provides guidance on how to sensitively support these pupils, and lessons are planned so as not to draw attention to any individual, thereby safeguarding pupils' privacy and wellbeing.

During online safety lessons, teachers foster a safe and supportive environment where all pupils feel comfortable to express their thoughts, ask questions, and seek help without fear of judgement or reprisal. Staff are alert to any disclosures or concerns arising during these lessons and follow the reporting procedures outlined in the Child Protection and Safeguarding Policy, using CPOMS to record and act upon any issues appropriately.

This comprehensive, responsive approach ensures that online safety is woven into the fabric of daily learning, equipping pupils with the critical skills and confidence they need to thrive in a digital world.

Use of Technology in the Classroom

A wide range of technology is employed to enrich learning experiences during lessons, including computers, laptops, tablets, interactive whiteboards, email, and cameras. These tools support interactive teaching and enable pupils to develop essential digital skills in a supervised and structured environment.

Before introducing any websites, tools, apps, or other online platforms in the classroom, or recommending them for use at home, class teachers thoroughly review and evaluate each resource for both educational value and safety. This diligence ensures that all materials are age-appropriate, relevant, and aligned with the school's safeguarding standards. Teachers also ensure that all internet-derived content is used in compliance with copyright law, demonstrating respect for intellectual property while modelling responsible digital citizenship.

When pupils engage with online materials during lesson time, they are always supervised by staff, with the level of oversight tailored to the age and ability of the class. This supervision helps protect pupils from potential online risks and provides guidance as they navigate digital environments. Through this careful approach,, Trust Education supports both the safe and effective integration of technology into everyday learning.

Use of Smart Technology

Pupils are permitted to bring personal mobile phones into school; this policy is in place as our pupils are often vulnerable, looked after children, and independently use public transport to travel to, and from Trust Education. Whilst pupils are allowed their phones on site, they are reminded that they are not allowed to use their phone on site and their phone must be kept in their bags, coats or passed to a member of staff to be kept in the mobile phone locker in the office. This is to minimise distractions, safeguard privacy, and maintain a focused learning environment. Nevertheless, the school recognises the importance of preparing pupils for responsible digital citizenship in a connected world. Where appropriate, pupils will be educated on the acceptable and appropriate use of personal devices, ensuring they understand the boundaries of safe and respectful behaviour both in and beyond the school setting.

Trust Education are committed

to staying informed about emerging devices, platforms, applications, trends, and digital threats. This proactive approach enables staff to adapt teaching and safeguarding strategies as the digital landscape evolves.

When educating pupils about the potential risks and appropriate uses of smart technology, the school employs the 4C's framework content, contact, conduct, and commerce. Lessons are designed to help pupils recognise harmful or inappropriate content, understand the implications of online contact, develop positive digital conduct, and be alert to risks associated with online commerce, including scams or in-app purchases. By embedding these principles into the curriculum and enforcing appropriate disciplinary measures where necessary, the school fosters a culture of critical thinking, digital safety, and responsible technology use.

Internet Access

To help maintain a safe and secure digital environment, all members of the school community are encouraged to access the internet via the school's network rather than through personal 3G, 4G, or 5G connections. The school's network is equipped with robust filtering and monitoring systems, ensuring internet usage is appropriate and aligned with safeguarding standards. By relying on the school's protected network, users benefit from these safety measures and help uphold the collective commitment to responsible online behaviour.

Filtering and monitoring online activity

In line with these practices, the governing board is committed to ensuring that the school's ICT network is equipped with robust filtering and monitoring systems that comply with national standards, including the DfE's 'Filtering and monitoring standards for schools and colleges'. Care is taken to avoid excessive restrictions

("over blocking") that could impede effective online teaching or the safeguarding curriculum.

The designated safeguarding lead (DSL) is responsible for assigning clear roles to manage these systems and verifying that they fulfil the school's safeguarding needs. Head of school, undertakes regular risk assessments to determine the suitability of the filtering and monitoring measures in place. These systems are selected based on pupils' ages, network usage patterns, and cost proportionality in relation to potential risks. Monthly reviews by ICT technicians ensure that the efficacy and relevance of filtering and monitoring arrangements are maintained.

Procedures are in place for adapting the filtering system: any requests for changes must be directed to the Head of school , with a joint risk assessment by the Head of School and DSL conducted before implementation. All alterations are logged by the Head of school and DSL. Reports of inappropriate online content are promptly investigated and actioned by the Head of school as needed.

Deliberate breaches of the filtering system are treated seriously. Such incidents are escalated to the DSL and are managed according to the severity of the breach and relevant school policies, including the Behaviour Policy for pupils and the Staff code of conduct for staff. If any material accessed is suspected to be illegal, it is reported immediately to the appropriate authorities, such as the Internet Watch Foundation (IWF), CEOP, or the police.

Monitoring applies to both the school's network and all school-owned devices. All users are informed about the nature and purpose of this monitoring, with concerns arising from monitoring addressed by the DSL in accordance with the Child Protection and Safeguarding Policy.

Network security

To further safeguard digital operations, the school maintains a suite of up-to-date technical security features. Filtering and monitoring company oversee the continuous maintenance of anti-virus software, ensuring all school devices are shielded against evolving threats. Firewalls are enabled at all times and are subject to regular review and timely updates by the filtering and monitoring company to preserve their effectiveness and integrity.

Staff and pupils are reminded to exercise caution by avoiding the download of unauthorised software and refraining from opening unfamiliar email attachments, which can introduce harmful malware. Any suspected malware or virus incident must be reported immediately to DSL for swift remediation.

System access protocols are strictly enforced: every staff member receives a unique username and private password for the school systems, while pupils, where applicable, are provided with their own individual credentials. Protecting the confidentiality of these credentials is a shared responsibility; passwords must not be

shared or disclosed, and users are never permitted to log in as another individual. Forgotten login details are to be reported directly to Head of school, who will facilitate secure access through alternative means. Any misuse or sharing of login information is promptly reported to the head of school, who determines and enacts appropriate disciplinary measures.

All users must also ensure devices and systems are locked when not in use, minimising the risk of unauthorised access and reinforcing the school's commitment to information security.

Emails

Access to and the use of emails is managed in line with the Data Protection Policy and Acceptable use of technology policies. Staff are provided with approved school email accounts, which are to be used exclusively for school purposes, both on site and when conducting school-related work outside regular hours. The use of personal email accounts on the school premises is strictly prohibited.

When handling sensitive or personal information, staff must only use secure and encrypted email channels to ensure confidentiality and data protection. Staff are responsible for blocking spam and junk mail, and any such incidents must be reported promptly to Head of school for investigation.

In line with the school's monitoring procedures, the system is equipped to detect inappropriate links, malware, and profanity embedded within emails. Both staff and pupils receive clear communication about this monitoring. Chain letters, unsolicited emails, and all correspondence from unknown sources must be deleted immediately without being opened, mitigating potential security risks.

Social networking for personal use.

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times. Staff receive annual training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils (past or present) or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are friends with a parent at the school, they will disclose this

to the DSL and Head of scholl and will ensure that their social media conduct relating to that parent is appropriate for their position in the school. Pupils, where appropriate, are taught how to use social media safely and responsibly through the online safety curriculum. Concerns regarding the online conduct of any member of the school community on social media are reported to the Head of school or DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy. The use of social media on behalf of the school is conducted in line with the Social Networking Sites. The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the head of school to access the school's social media accounts. All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

The school website

Head of school is responsible for the overall content of the school website, they will ensure the content is appropriate, accurate, up-to-date and meets government requirements. The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the appropriate consent has been received.

Personal devices are not permitted to be used in the following locations:

• Toilets

• Changing rooms/shower room

• Corridors

• Classrooms when pupils are present

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils. Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the code of conduct policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, Head of school will inform the police and action will be taken Pupils are not permitted to use their personal devices in school. The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use. Where a pupil uses accessibility features on a personal device to help them access education e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, or for medical purposes e.g. management of diabetes, the arrangements and rules for conduct for

this are developed and managed on a case-by-case basis. Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL or Head of school.

Monitoring and review

The school recognises that the online world is constantly evolving. As such, the Designated Safeguarding Lead (DSL), Head of school and governors, carry out termly light-touch reviews of this policy to assess its effectiveness. A full review of the policy is conducted annually by the governing board, head of school, and DSL, and also in response to any significant online safety incidents. The next scheduled full review is set for September 2026. Any changes made to this policy will be communicated to all members of the school community.

Policy Lead	Melissa Wainman Director of Education
Date:	15th September 2025
Policy Review Date:	September 2026
Version:	1
Approval:	Trust-Education Group Board of Governors