Online Safety Policy

TEAM Education Trust

Policy approved by:	Trust Board	Date: 14 October 2025
Last reviewed on:	17 Sept 2025	
Next review due by:	1 September 2026	
List of associated policies/documents:	TEAM Anti-bullying policy TEAM Staff Code of Conduct Policy TEAM Student Behaviour Policy TEAM Safeguarding and Child Protection policy TEAM Education Trust GDPR Policies (1-12) TEAM Virtual Meeting Policy TEAM IT Policy TEAM AI Policy TEAM curriculum policies & plans to include Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)	

Version History

Version	Date	Detail	Author
1	01.05.22	New Policy	PLI
2	22.05.23	Amendments: Section 4.1 Identify and assign roles and responsibilities to manage your filtering and monitoring systems as recommended by the DFE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) Section 4.2 DFE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring. Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective. You may need to ask your filtering provider for system specific training and support. The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring. Section 4. DFE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) Filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning Review filtering and monitoring provision at least annually Section 4.7 Governing Body The Governing Body will: Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met. To do this, they should identify and assign: a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met the roles and responsibilities of staff and third parties, for example, external service providers Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is	

		reviewed, which can be part of a wider online safety review, at least annually. Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually. Governing bodies and proprietors need to support the senior leadership team to procure and set up systems which meet this standard and the risk profile of the school or college. Ensure effective monitoring strategies that meet the safeguarding needs of the school. Governing bodies and proprietors should support the senior leadership team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school or college. DFE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) Section 5.1 Utilise resources such as: Teaching online safety in schools - GOV.UK (www.gov.uk) Section 7.3 DFE digital standards updated 29 March 2023 inform this section: Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)	
3	26.02.24	Updated the name of the policy that is connected to – title page Punctuation altered/corrected on the following pages 5-9,11, 14-28, 30, 31 Updated title of guidance P5 Updated four areas of risk not three P6 Amended 'delete comment' P6 Added internet service provider P16 Listed concerns of monitoring P16 Updated GDPR reference P16 Updated policy reference was separate list now under IT policy P17 Updated safeguarding details P18 Learning platform details added P20 Class DoJo Added P20 Added social media name P22 Amended 'delete comment' P22 Spelling WI-FI P23 Amended paragraph to 'delete comment' and added details P23 Amended the release mobile phone comment to refer to desecration of the schools P24	EJK

		Content page numbers updated to match 4.7 Added to contents 4.7 Governing body section 7.9.1 Added to contents 7.9.2 Added to contents	
4	24.02.25	Updated the list of associated policies P6 Updated link to additional DfE guidance Updated page numbers on content page including adding 7.9.1, 7.9.2 and updating the numbers 11.7, 11.8, 11.9 both on contents page and sections on policy 11.6 Added AI update P31 8.3 Updated name 'Twitter' to 'X' P23	EJK
5	17.09.25	1 - Updated the definition of content to explicitly include misinformation, disinformation and conspiracy theories as identified in KCSIE 2025 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7 - Added additional roles and responsibilities in relation to Generative AI for Leadership, DSL, Learners, Parents/carers and governing bodies 5.1, 5.2 - Updated education and engagement to include teaching about misinformation, disinformation, conspiracy theories and deep fakes 7.3 - Reference to monitoring updated and added DfE Plan Technology for Your School self-assessment tool 10-11 – Added line about online harm from misinformation etc.	EJK

Contents

1. Policy Aims

This online safety policy has been written by T.E.A.M. Education Trust, involving staff, learners and parents/carers, building on the Derbyshire County Council's online safety policy template.

It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' , Early Years and Foundation Stage, 'Working Together to Safeguard Children' and Working Together to Improve School Attendance. It also refers to the DfE's guidance on protecting children from radicalisation

The purpose of this online safety policy is to:

- Safeguard and protect all members of TEAM Education Trust schools' community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, including in the delivery of remote learning, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

This school identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material. "The definition of online content risk now explicitly includes misinformation, disinformation and conspiracy theories, as identified in KCSIE 2025"
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm
- Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Policy Scope

T.E.A.M. Education Trust believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

T.E.A.M. Education Trust identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

T.E.A.M. Education Trust believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

3. Monitoring and Review

Technology in this area evolves and changes rapidly. Each Trust school will review this policy at least annually.

The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

To ensure they have oversight of online safety, the principal will be informed of online safety concerns, as appropriate.

The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.

Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

The school's Designated Safeguarding Lead (DSL) has lead responsibility for online safety. Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall, the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.

T.E.A.M. Education Trust recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team

The leadership management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and/or acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure parents are directed to online safety advice and information
- Provide information on a school's website for parents and the community
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.

- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Ensure any use of generative AI technology complies with DfE product safety expectations for generative tools (2025) particularly regarding safeguarding, logging and transparency
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- As recommended by the DfE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
    - Identify and assign roles and responsibilities to manage your filtering and monitoring systems
    - They should make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually.
- The review should be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider and involve the responsible governor. The results of the online safety review should be recorded for reference and made available to those entitled to inspect that information.
- Your IT service provider may be a staff technician or an external service provider.

4.2 The Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date, and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- DSLs must also monitor risks arising from misinformation, disinformation and conspiracy theories
- Report online safety concerns, as appropriate, to the setting management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- DfE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and

monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
    - The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.
    - Management of filtering systems requires the specialist knowledge of both safeguarding and IT staff to be effective. You may need to ask your filtering provider for system specific training and support.
    - The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.

4.3 Members of Staff

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Staff need to recognise safeguarding risks linked to generative AI (deepfakes, impersonation, harmful or biased content)
- Identify students who are involved in cybercrime, or those who are technically gifted and talented and are at risk of becoming involved in cybercrime and make a Cyber Choices referral.

4.4 Staff who manage the technical environment

It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the DSL and leadership team, these include password policies and encryption; but not exclusive, to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.
- Technical staff must ensure any AI tools/platforms comply with DfE Generative AI Product Safety Expectations (2025)
- DfE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and

monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)
    - Filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning
    - Monitoring strategies should help detect risks from AI-enabled fraud, identity misuse or manipulated content
    - Review filtering and monitoring provision at least annually

4.5 Learners

It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.
- Learners will also be supported to understand the risks posed by misinformation, disinformation, conspiracy theories, and AI-generated content such as deepfakes or impersonation. They will be encouraged to question online sources, report concerns promptly, and recognise the importance of attendance in reducing safeguarding risks

4.6 Parents and Carers

It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media
- Abide by the home-school agreement and/or acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately. These include Class Dojo, Tapestry and Evidence for Learning.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.
- Parents and carers will receive guidance on the risks of misinformation, disinformation, conspiracy theories and AI-generated content. They will be encouraged to talk with their children about these risks, model critical thinking when online, and reinforce safe behaviours at home. Parents and carers are reminded that absence from education can increase safeguarding risks, including online risks, and are expected to support good attendance alongside safe and appropriate use of technology.

4.7 Governing Body

The Governing Body will:

- Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.
- To do this, they should identify and assign:
    - a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met

    - the roles and responsibilities of staff and third parties, for example, external service providers
- Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually.
- Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually.
- Governing bodies and proprietors need to support the senior leadership team to procure and set up systems which meet this standard and the risk profile of the school or college.
- Must have an oversight of generative AI tools used in school ensuring they are risk assessed and do not expose learners to harmful or unsafe content
- Ensure effective monitoring strategies that meet the safeguarding needs of the school.

Governing bodies and proprietors should support the senior leadership team to make sure effective device monitoring is in place which meets this standard and the risk profile of the school or college. DfE's Meeting digital and technology standards in schools and colleges guidance - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

5. Education and Engagement Approaches

5.1 Education and engagement with learners

The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Include teaching about misinformation, disinformation, conspiracy theories and deepfakes
- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
- Displaying acceptable use posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology when appropriate
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.
- Utilise resources such as:
- Teaching online safety in schools - GOV.UK (www.gov.uk)

5.2 Vulnerable Learners

Settings should include specific information in this section about how their community's needs have been identified and what action has been taken e.g. specific filtering requirements for children with EAL or SEND. This is especially important for special schools or settings with specialist units; policies should reflect the settings circumstances.

T.E.A.M. Education Trust recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Each school in TEAM Education Trust will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners. When implementing an appropriate online safety policy and curriculum T.E.A.M. Education Trust will seek input from specialist staff as appropriate, including the SENCO, Looked After Child Designated Teacher. Training and engagement with staff.

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff, including governors where relevant to their role on a regular basis, with at least annual updates.
- Online risk may disproportionately affect children in kinship care, children with social workers and those persistently absent from education (KCSIE 2025)
- Settings should identify how this will be achieved here; for example, as part of existing safeguarding and child protection training/updates or within separate or specific online safety sessions.
- This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues, or other members of the community.

5.3 Awareness and engagement with parents and carers

T.E.A.M. Education Trust recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.

- This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes, and sports days.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

T.E.A.M. Education Trust recognises that the internet is a constantly changing environment with new apps, devices, websites, and material emerging at a rapid pace.

We will:

- Regularly review the methods used to identify, assess, and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images, or videos which could cause harm, distress, or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- T.E.A.M. Education Trust uses a wide range of technology. This includes access to: Computers, laptops, and other digital devices
- Internet which may include search engines and educational websites
- Learning platform/intranet
- Email (where appropriate and permitted for use as part of the curriculum)
- Games consoles and other games-based technologies
- Digital devices with cameras (iPads and laptops), web cams and video cameras

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

Settings should list the specific measures in place e.g. for tablets, if mobile device management software will be used, how access will be recorded and how this will be enforced.

Members of staff will always evaluate websites, tools, and apps fully before use in the classroom or recommending for use at home.

The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

Settings should list search tools suggested for staff and learners to use. Examples include SWGfL Squiggle, Dorling Kindersley find out, Google Safe Search or CBBC safe search.

Google Safe Search, Youtube Restrict: Strict Mode and blocking of Youtube from Chrome browsers are implemented by policy through our device management platforms.

We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.

Supervision of learners will be appropriate to their age and ability.

Early Years Foundation Stage and Key Stage 1
Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

Key Stage 2
Learners will use age-appropriate search engines and online tools.
Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

Key Stage 3, 4, 5 (where appropriate)
Learners will be appropriately supervised when using technology, according to their ability and understanding.

7.2 Managing Internet Access

We will maintain a record of users who are granted access to our devices and systems.

All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

We will carry our regular audits and audit activity to help identify pupils trying to access sites to establish any vulnerabilities and offer advice, support, and react accordingly.

7.3 Filtering and Monitoring

DFE digital standards updated 10 March 2025 inform this section: Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk).

Note: A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

Other document support around Filtering and Monitoring can be found here: DfE's Plan Technology for Your school self-assessment tool

T.E.A.M. Education Trust governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.

The governors and leaders are aware of the need to prevent "over blocking," as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.

Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.

The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.1 Filtering

Education broadband connectivity is provided through (Name of Internet Service Provider).

We use (Name of Filtering System) which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming, and sites of an illegal nature. (Edit and amend to reflect setting decisions e.g. add here what categories are or are not blocked)

The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

We work with EMPSN to ensure that our filtering policy is continually reviewed.

If learners discover unsuitable sites, they will be required to:

- Insert details of the procedure here e.g. turn off monitor/screen and report the concern immediate to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Derbyshire Police or CEOP.

7.3.2 Monitoring

We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:

- Ensuring anti-malware software applications are installed and enabled on all endpoints, virus signature databases are always up-to-date, and files are set to be scanned on-access.

- Automated suspicious/unusual behaviour event notifications including the deploying a monitored 'honeypot' folder at the top of critical data directories that serves as an early warning.
- Deploying robust email filtering systems to block, quarantine or flag suspicious emails.
- Reporting of suspicious emails or events by school staff.
- Must include risks linked to AI tools (e.g. harmful deepfake or impersonation material)

7.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred, and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

Full information can be found in our GDPR policy section, relating to IT security and Data protection

7.5 Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection and malware solutions deployed to all Windows devices and configured for regular updates.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Blocking staff from downloading unapproved software to work devices
- Use of Microsoft Safe Links for review of all embedded links in emails
- Virus and malware checks within the email solution and on the endpoint device
- Backup of our online data held in Office365 Exchange, Onedrive, Sharepoint and Teams and testing of restoration processes
- Segregation of school and guest networks through the use of VLAN's.
- Firewall and ACL rules annually reviewed.
- Appropriate use of user logins and passwords to access our network.
- Specific user logins and passwords will be enforced for all but the youngest users. (Note: this should be in place for all except Early Years and Foundation Stage children and some learners with SEND)
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found within our IT policy

7.6 Managing the Safety of our Website

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE). (This statement is specific to schools; however, an up-to-date website is viewed as good practice for other settings).

We will ensure that our website complies with guidelines for publications including, accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.

Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email, and telephone number.

The administrator account for our website will be secured with an appropriately strong password.

We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

7.8 Managing Email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.

The forwarding of any chain messages/emails is not permitted.

Spam or junk mail will be blocked, and reports can be monitored by the Trust IT team.

All email is accessed through some form of encryption technology in transition and at rest. All email communication will be sent with implicit encryption, and enhanced encryption used when sensitive or personal information is sent using explicit encryption (where recipients cannot remove encryption) and data loss prevention DLP.

Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the community will immediately tell Nicola Rees TEAM Safeguarding lead, if they receive offensive communication, and this will be recorded in our safeguarding files/records.

We will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

7.8.1 Staff email

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners, and parents.

Members of staff will refer to and adhere to the acceptable use policy and any other policy where staff use of mobiles is referred to.

7.8.2 Learner email

Learners will use provided email accounts for educational purposes.

Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

Whole class or group email address are not permitted for communication outside of the setting.

All individual learner email accounts are not permitted for communication with addresses outside of the setting.

7.9 Educational use of Videoconferencing and/or Webcams

T.E.A.M. Education Trust recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.

All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.

Videoconferencing details will not be posted publicly.

All invitations to attend video conferencing should be sent explicitly to the invited attendee.

Where large groups may attend video conference session a member of staff will monitor and approve/reject attendees waiting in the lobby to join.

All meetings held using video conferencing technology will have a lobby assigned and internal attendees only can bypass the lobby with all external attendees required to wait in the lobby until permitted into the meeting.

Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

7.9.1 Users

Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.

Learners will ask permission from a member of staff before making or answering a videoconference call or message.

Videoconferencing will be supervised appropriately, according to the learner's age and ability.

Video conferencing will take place via official and approved communication channels following a robust risk assessment.

Only key administrators will be given access to videoconferencing administration areas or remote-control pages.

The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.

If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.

We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

7.10 Management of Learning Platforms

The schools within the trust use a range of learning platforms such Rock Stars, Lexia, Maths flex, although these differ between the sites.

Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.

Only current members of staff, learners, and parents (where appropriate) will have access to the LP.

When staff and/or learners leave the setting, their account will be disabled or transferred to their new establishment.

Learners and staff will be advised about acceptable conduct and use when using the LP.

All users will be mindful of copyright and will only upload appropriate content onto the LP.

Any concerns about content on the LP will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- If the user does not comply, the material will be removed by the site administrator.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement.
- A learner's parents/carers may be informed.
- If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

7.11 Management of Applications (apps) used to Record Children's Progress

We use Class DoJo to track learners progress and share appropriate information with parents and carers.

The principal is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior

to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
To safeguard learner's data:

- Only teacher issued managed devices will be used for apps that record and store learners' personal details, attainment, or photographs.
- Personal staff mobile phones or devices will not be permitted to access or upload content to any apps which record and store learners' personal details, attainment, or images.
- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

The expectations' regarding safe and responsible use of social media and remote learning platforms applies to all members of T.E.A.M. Education Trust community.

Members of staff will refer to and adhere to the school's social media policy and any other policy where the staff use of social media is referred to.

We will control learner and staff access to social media whilst using setting provided devices and systems on site.

Concerns regarding the online conduct of any member of T.E.A.M. Education Trust community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour, and child protection policies.

8.2 Learners Personal Use of Social Media

Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age-appropriate sites and resources.

We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.

Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.

Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games, or tools.
Learners will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.

- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

8.3 Official Use of Social Media

Official social media channels are:

- X

The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

The official use of social media as a communication tool has been formally risk assessed and approved by the headteacher/manager.

Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.

Staff use setting provided email addresses to register for and manage any official social media channels.

Official social media sites are suitably protected and, where possible, run and/or linked to/from our website.

All communication on official social media platforms will be clear, transparent, and open to scrutiny.

Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

Any official social media activity involving learners will be moderated possible. (If appropriate)

Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

9. Use of Personal Devices and Mobile Phones

T.E.A.M. Education Trust recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff, and parents/carers, but technologies need to be used safely and appropriately within the setting.

9.1 Staff Use of Personal Devices and Mobile Phones

Members of staff will refer to and adhere to the school's acceptable use policy and any other policy where the staff use of personal devises and mobile phones is referred to.

Staff members devices will not be permitted to access the main school network, only upon request will they be permitted to connect to a guest Wi-Fi solution that is segregated from the main school network.

9.2 Learners Use of Personal Devices and Mobile Phones

Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

T.E.A.M. Education Trust expects learners' personal devices and mobile phones to be kept in a secure place, switched off, kept out of sight during lessons and while moving between lessons.

If a learner needs to contact his/her parents or carers they will be allowed to use a setting phone.

Parents are advised to contact their child via the setting office; exceptions may be permitted on a case-by-case basis, as approved by the headteacher/manager.

Mobile phones or personal devices will not be used by learners during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.

The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.

Mobile phones and personal devices must not be taken into examinations.

Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.

Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).

Searches of mobile phone or personal devices will only be carried out in accordance with DfE guidance and our policy. (Appropriate for schools only and must link to appropriate policy. See www.gov.uk/government/publications/searching-screening-and-confiscation)

Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted if it contravenes our policies. (Appropriate for schools only and must link to appropriate policy. See www.gov.uk/government/publications/searching-screening-and-confiscation)

Mobile phones and devices that have been confiscated will be released to parents or carers at the discretion of the school

If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.3 Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.

We will ensure appropriate signage and information is displayed and provided to inform parents, carers, and visitors of expectations of use.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or headteacher/manager of any breaches our policy.

9.4 Officially provided mobile phones and devices (Use If provided)

Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.

Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies within the trust relating to BYOD.

10. Responding to Online Safety Incidents and Concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including, breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community will be made aware of the availability of the Cyber Choices early intervention programme for individuals who are involved in cybercrime, or those who are gifted and talented and are at risk of becoming involved in cybercrime.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.

Learners, parents, and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents, carers, and learners to work in partnership to resolve online safety issues.

After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

We will refer to the flow chart on responding to incidents, made available

Where there is suspicion, that illegal activity has taken place, we will follow the local safeguarding procedures which will include Police using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or headteacher/manager will speak with Call Derbyshire/ Derbyshire Police first to ensure that potential investigations are not compromised.

10.1 Concerns about Learners Welfare

The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.

The DSL (or deputy) will record these issues in line with our child protection policy.

The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Derby and Derbyshire Safeguarding Children Partnership thresholds and procedures.

We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

Our school/ setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" guidance and part 5 of 'Keeping children safe in education'.

T.E.A.M. Education Trust recognises that sexual violence and sexual harassment between children can take place online. Examples may include non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

T.E.A.M. Education Trust recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

T.E.A.M. Education Trust also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

T.E.A.M. Education Trust will ensure that all members of the community are made aware of the potential social, psychological, and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
- If content is contained on learners electronic devices, they will be managed in accordance with the DfE ‘searching screening and confiscation’ advice.
- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting, and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children’s Social Work Service and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police service first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery ("Sexting")

T.E.A.M. Education Trust recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery."

T.E.A.M. Education Trust will ensure that all members of the community are made aware of the potential social, psychological, and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods. (Identify resources as appropriate)

We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policies and the relevant Derbyshire Safeguarding Child Board's procedures.
- Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Store the device securely.
- If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of learners involved, including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.

- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

T.E.A.M. Education Trust will ensure that all members of the community are aware of online child sexual abuse, including, exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

T.E.A.M. Education Trust recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).

We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff, and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant Derbyshire Safeguarding Child Board's procedures.
- If appropriate, store any devices involved securely.
- Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the “Make a Report” button at: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire police by using 101.

If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Derbyshire police using 101 unless immediate concerns and 999 will be used by the DSL (or deputy).

If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Derbyshire Police first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

T.E.A.M. Education Trust will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls, and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire Police using 101.

If made aware of IIOC, we will:

- Act in accordance with our child protection policy and the relevant Derby City & Derbyshire Safeguarding Children Partnership Safeguarding procedures.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Derbyshire police or the LADO.

If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy) is informed.

- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the Derbyshire police via 101 (999 if there is an immediate risk of harm) and Children's Services using Call Derbyshire (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the headteacher/manager is informed in line with our managing allegations against staff policy immediately and without any delay.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at T.E.A.M. Education Trust.

Full details of how we will respond to cyberbullying are set out in our anti-bullying policy within the TEAM Trust policy folder.

11.6 Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are not widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

T.E.A.M Education Trust recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI include someone's likeness.

T.E.A.M Education Trust will treat any use of AI to bully pupils very seriously, in line with our Anti Bullying/Student behaviour policies.

T.E.A.M Education Trust will respond to online harms including those arising from misinformation, disinformation and conspiracy theories, recognising their potential safeguarding impact

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out risk assessment where new AI tools are being used by the school/trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

Any use of Artificial Intelligence should be carried out in accordance with our AI policy.

11.7 Online Hate

Online hate content, directed towards or posted by specific members of the community will not be tolerated at T.E.A.M. Education Trust and will be responded to in line with existing policies, including anti-bullying and behaviour.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

The Police will be contacted if a criminal offence is suspected.
If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Derbyshire police and or the safer Derbyshire website https://www.saferderbyshire.gov.uk/home.aspx

11.8 Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. Monitoring systems are in place and are outlined in our IT policy to ensure that students are protected online.

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy and Derbyshire prevent pathway which may include a referral into Channel.

If we are concerned that member of staff may be at risk of radicalisation online, the headteacher/manager will be informed immediately, and action will be taken in line with the child protection and allegations policies.

11.9 Cybercrime

Cybercrime incidents and offences will be responded to in line with our existing behaviour policies.

We will respond to concerns that our students are involved, or at risk of becoming involved, in cybercrime, even if it takes place off site.

We will make a Cyber Choices referral for early intervention, as per the https://www.saferderbyshire.gov.uk/what-we-do/cyber-crime/reporting-cybercrime/reporting-cybercrime.aspx

If we are concerned that a child is being exploited as a result of their technical skills, we will follow the Children at Risk of Exploitation (CRE) procedure and the CRE Risk Assessment Toolkit

https://www.saferderbyshire.gov.uk/what-we-do/cyber-crime/reporting-cybercrime/digital-mot/digital-mot.aspx

12. Useful Links for Educational Settings

Support and Guidance for Educational Settings

Derby City & Derbyshire Safeguarding Children Partnership online procedures DDCSP: http://derbyshirescbs.proceduresonline.com/

Derbyshire Police:
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Derbyshire Police via 101

LADO
By referral into Professional.Allegations@derbyshire.gov.uk
Form found here http://derbyshirescbs.proceduresonline.com/docs_library.html
Call Derbyshire (Starting Point)
Immediate risk of harm phone 01629 533190
For all other referrals complete an online form https://www.derbyshire.gov.uk/social-health/children-and-families/support-for-families/starting-point-referral-form/starting-point-request-for-support-form.aspx
For professional advice phone 10629 535353
National Links and Resources for Educational Settings
CEOP: www.thinkuknow.co.uk www.ceop.police.uk
Childnet: www.childnet.com
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
NSPCC: www.nspcc.org.uk/onlinesafety
ChildLine: www.childline.org.uk
Net Aware: www.net-aware.org.uk
The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
UK Safer Internet Centre: www.saferinternet.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
360 Safe Self-Review tool for schools: www.360safe.org.uk
National Links and Resources for Parents/Carers
Action Fraud: www.actionfraud.police.uk
CEOP: www.thinkuknow.co.uk www.ceop.police.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
NSPCC: www.nspcc.org.uk/onlinesafety
ChildLine: www.childline.org.uk
Net Aware: www.net-aware.org.uk
The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
UK Safer Internet Centre: www.saferinternet.org.uk