ELSTON HALL
Learning Trust

Online Safety Policy

Updated: February 2026

Approved by Trustees: 10 February 2026

Review Date: February 2027

CONTENTS

Scope of the Online Safety Policy

This policy applies to all members of the Trust and school communities (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of Trust and school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Elston Hall Learning Trust will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

The Trust Online Safety Policy:

- Outlines the commitment of Elston Hall Learning Trust to safeguard members of the Trust and school communities online, in accordance with statutory guidance and best practice including 'Keeping Children Safe in Education' 2025, 'Working Together to Safeguard Children' and DfE Safeguarding and remote education. The policy should be read in conjunction with Ofsted's 'Review of sexual abuse in schools and colleges' and UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people and DfE Behaviour in Schools 2022.
- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the schools will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is monitored at regular intervals
- is made available to staff at induction and through normal communication channels

Policy development, monitoring and review

This Online Safety Policy has been developed by:

- *Headteachers and Trust Leaders*
- *Designated safeguarding leads (DSL)*
- *Online Safety Leads*
- *Trust's Digital Strategy and Estates Manager*
- *staff – including teachers/support staff/technical staff*
- *Trust's DPO*

The Trust will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
    - learners
    - parents and carers
    - staff

Responsibilities

To ensure the online safeguarding of members of our Trust and school communities it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the Trust and its schools.

Headteacher and senior leaders

- Trust Leaders and Headteachers have a duty of care for ensuring the safety (including online safety) of members of the Trust and school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- At schools, the headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Headteachers/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

- Headteachers/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteachers/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteachers/senior leaders will work with the responsible Trustee, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Trustees

Trustees are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Designated Safety Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant Advisory School Committee meetings
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling themand deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Leads

The Online Safety Leads will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), (where these roles are not combined)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the Trust online safety policies/documents

- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/those in governance roles/parents/carers/learners
- liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- Cross-curricular links
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations

- all digital communications with learners, parents and carers and others should be on a professional level *and only carried out using official school systems and devices (where staff use AI, they should only use Trust-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements*
- they immediately report any suspected misuse or problem to *the DSL* for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- they adhere to the Trust's Data Protection policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

IT Provider

The Trust has a technology service provided by an external contractor. It is the responsibility of the Trust to ensure that the provider carries out all the online safety measures that the Trust's obligations and responsibilities require, in line with this policy.

The IT Provider is responsible for ensuring that:

- the Trust's technical infrastructure is secure and is not open to misuse or malicious attack
- the Trust meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to DSLs for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- *monitoring systems are implemented and regularly updated as agreed in school policies*

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Trust's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

Our Trust / schools will take every opportunity to help parents and carers understand these issues through:

- publishing this policy on the Trust website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA)

- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- *reinforcing the online safety messages provided to learners in school.*

Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of Trust / school life i.e.

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence
- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned Trust and school mechanisms.
- *Where Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.*

Acceptable use

The Trust has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

This policy and acceptable use agreements define acceptable use at the Trust and its schools. The acceptable use agreements will be communicated/re-enforced through:

- student induction
- staff induction
- posters/notices around where technology is used

- communication with parents/carers
- built into education sessions
- Trust and school websites
- peer support

User Actions which are unacceptable and illegal

Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to any illegal activity. For example:

- Child sexual abuse imagery*
- Child sexual abuse/exploitation/grooming
- Terrorism
- Encouraging or assisting suicide
- Offences relating to sexual images i.e., revenge and extreme pornography
- Incitement to and threats of violence
- Hate crime
- Public order offences - harassment and stalking
- Drug-related offences
- Weapons / firearms offences
- Fraud and financial crime including money laundering

N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges

Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990):

- Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)
- Gaining unauthorised access to school networks, data and files, through the use of computers/devices
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)
- Disable/Impair/Disrupt network functionality through the use of computers/devices
- Using penetration testing equipment (without relevant permission)

N.B. Schools would need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit

to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information here

User Actions which are Unacceptable in the Trust and Schools

Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:

- Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)
- Promotion of any kind of discrimination
- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school
- Infringing copyright and intellectual property (including through the use of AI services)
- Unfair usage (downloading/uploading large files that hinders others in their use of the internet)
- Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute

For staff and adults, consideration should be given for the following activities when undertaken for non-educational purposes.				
For CHILDREN, each category would be 'Not allowed'				
	Not allowed	**Allowed**	**Allowed outside work hours**	**Allowed for selected staff**
Online Gaming	x			
Online Shopping/commerce	x			
File Sharing	x			
Messaging / chat	x			
Entertainment streaming (Netflix etc)	x			
Video Broadcasting (YouTube/ TikTok/ Twitch)	x			

Mobile Phones to be brought to school *(children's phones can be brought to school but kept in the office)*			x	
Taking photos on mobile phones / cameras / smart watches	x			
Use of other personal devices, e.g.: tablets, gaming devices	x			
Use of personal email in school or on school network			x	
Use of school email for personal emails	x			
Use of AI services that have not been approved by the Trust	x			

When using communication technologies, the Trust considers the following as good practice:

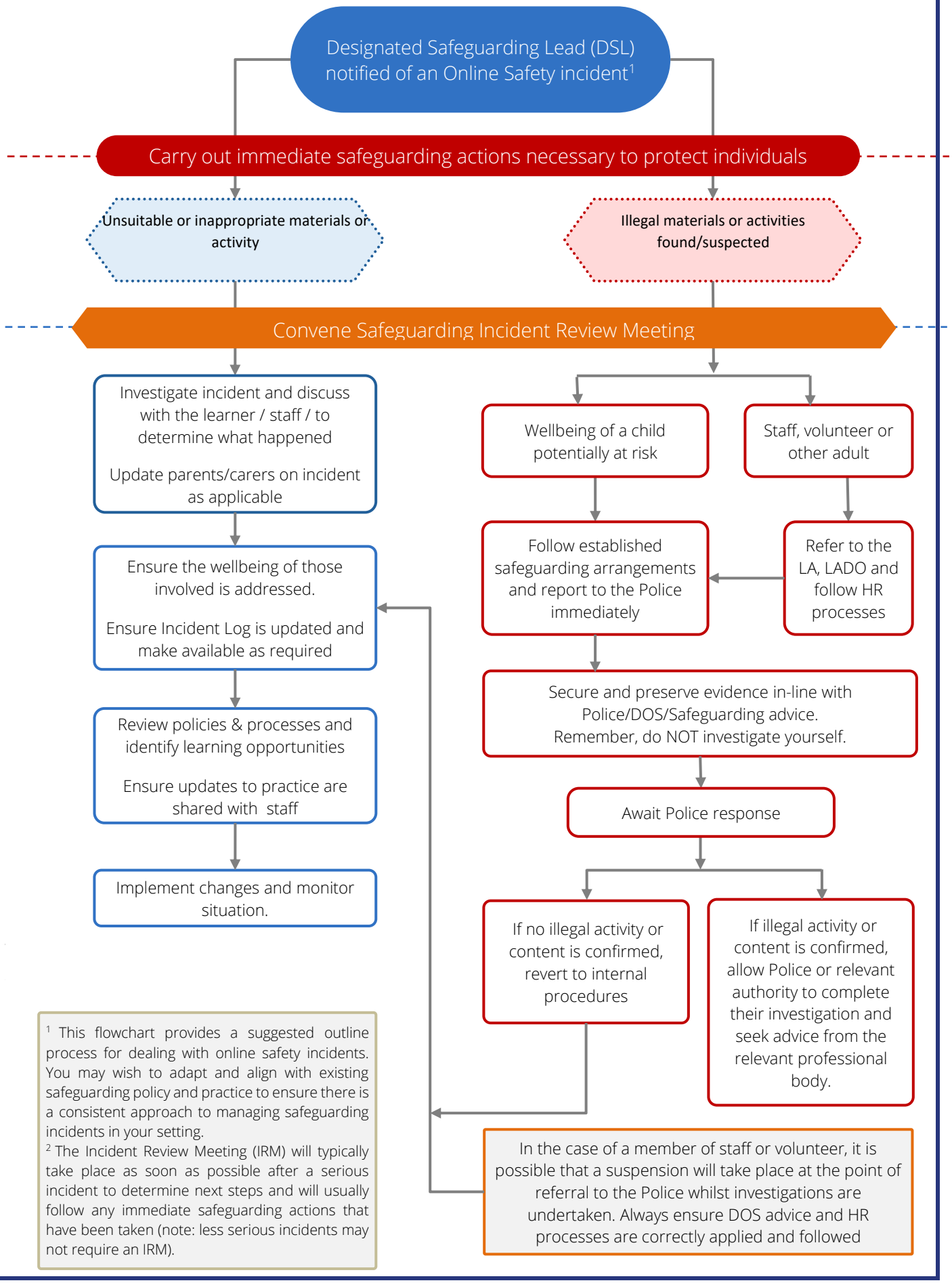
- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the Trust / school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the Trust / school and its community
- users should immediately report to a nominated person – in accordance with the Trust policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.*

Reporting and responding

The Trust / school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The Trust / school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the Trust's whistleblowing, complaints and managing allegations policies.
- all members of the Trust / school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

- any concern about staff misuse will be reported to the Trust Leader or Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Trustees and the Trust
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

Trust / School actions

It is more likely that the Trust / school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Trust / school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Learner Actions

Incidents	Refer to class teacher	Refer to Headteacher	Refer to Police/Social Work	Refer to IT technical support for advice/action	Inform parents/carers	Remove device/ network/internet access	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		x	x		x	x	x	x
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords		x		x	x	x	x	x
Corrupting or destroying the data of other users.		x		x	x	x	x	x
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		x			x		x	x

Unauthorised downloading or uploading of files or use of file sharing.		x			x		x	x
Using proxy sites or other means to subvert the school's filtering system.		x		x	x	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident.		x		x	x		x	x
Deliberately accessing or trying to access offensive or pornographic material.		x		x	x	x	x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		x		x	x	x	x	x
Unauthorised use of digital devices (including taking images)		x	x	x	x	x	x	x
Unauthorised use of online services		x			x	x	x	x
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		x			x	x	x	x
Continued infringements of the above, following previous warnings or sanctions.		x			x	x	x	x

Responding to Staff Actions

Incidents	Refer to Headteacher / Trust Leader	Refer to /MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	x	x	x	
Actions which breach data protection or network / cyber-security rules.	x	x		x
Deliberately accessing or trying to access offensive or pornographic material	x	x		x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x		x
Using proxy sites or other means to subvert the school's filtering system.	x	x		x
Unauthorised downloading or uploading of files or file sharing	x	x		x
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)	x	x		x
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	x	x		x
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	x	x		

Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	x	x		
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	x	x		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	x	x		
Actions which could compromise the staff member's professional standing	x	x		
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	x	x		
Failing to report incidents whether caused by deliberate or accidental actions	x	x		
Continued infringements of the above, following previous warnings or sanctions.	x	x		

The use of Artificial Intelligence (AI) systems in the Trust and our Schools

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and Trust and school operations; ensuring all use is safe, ethical and responsible is essential.

See AI policy for full details.

Online Safety Education Programme

Online safety is a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment

- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
- learners should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum.
- staff should act as good role models in their use of digital technologies the internet and mobile devices.
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites / tools (including AI systems) the learners visit.
- it is accepted that from time to time, for good educational reasons, learners may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- the online safety education programme is relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Learners

The Trust acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion
- appointment of digital leaders/anti-bullying ambassadors/peer mentors
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns.
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff/volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the Trust / school's annual safeguarding, data protection and cyber-security training for all staff – all staff and IT users must also complete annual cyber security training for satisfying Trust insurance requirements
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the Trust online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Families

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day

- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority/MAT

Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- *providing online safety information via their website and social media for the wider community*

Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school ensures that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The Trust's filtering and monitoring provision (Lightspeed) is agreed by senior leaders, Trustees and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader and the Designated Safeguarding Lead, in particular when a safeguarding risk is identified or there is a change in working practice.

Filtering

Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education.

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video

- Headteacher and trustees are responsible for ensuring these standards are met. Roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined
- the Trust and schools manage access to content across its systems for all users and on all devices using the Trust's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- There are regular checks of the effectiveness of the filtering systems.
- Devices that are provided by the Trust have school-based filtering applied irrespective of their location.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with Trust policy and practice.

Monitoring

Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything.

The Trust follows the UK Safer Internet Centre Appropriate Monitoring guidance.

The Trust has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users:

- The Trust monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours.
- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- monitoring enables alerts to be matched to users and devices (where possible).

Technical Security

The Trust technical systems will be managed in ways that ensure that the school meets recommended standards in the DfE Technical Standards for Schools and Colleges:

- responsibility for technical security resides with Chief Executive / school headteachers who may delegate activities to identified roles.
- All Trust systems have a permission-based access control model in place, clearly defining access rights to Trust and School systems and devices.
- All users (staff and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all Trust networks, devices and system will be protected by secure passwords.
- the administrator passwords for school systems are retained by the Trust's IT provider.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of Trust technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The Trust infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,

- The IT service provider is responsible for ensuring that all software purchased by and used by the Trust / schools is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of Trust / school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the Trust network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a Trust or school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place
- guest users are provided with appropriate access to school systems based on an identified risk profile.
- systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured.
- Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
- dual-factor authentication is used for sensitive data or access outside of a trusted network, where required
- where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.
- Where AI services are used, the Trust / school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias

Mobile technologies

The Trust acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The Trust allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	No	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	N/A	N/A	N/A	No	No	Yes
Some network access	N/A	N/A	N/A	No	No	No

School owned/provided devices:

- All Trust / school devices are managed though the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- any designated mobile-free zone is clearly signposted
- personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from school is clearly defined and expectations are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

Personal devices:

- there is a clear policy covering the use of personal mobile devices on school premises for all users

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as confidentiality, child protection, data security and acceptable use of technology.
- Staff will be advised to:
    - keep mobile phones and personal devices in a safe and secure place (e.g. locked in a locker/drawer) during lesson time.
    - keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - Smart Watches should be on silent mode with no interaction allowed in working hours
    - ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
    - not use personal devices during teaching periods unless prior permission has been given by the Headteacher such as in emergency circumstances.
    - ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Staff will only use school provided equipment (not personal devices):
    - to take photos or videos of learners in line with our image use policy.
    - to work directly with learners during lessons/educational activities
    - to communicate with parents and carers.

- Where remote learning activities are required staff will use school provided equipment.
- If a member of staff breaches our policy, action will be taken in line with our Disciplinary Policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

    - where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.
    - where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available.
    - use of personal devices for Trust / school business is defined in the Trust's acceptable use policy. Personal devices commissioned onto the school network are segregated effectively from school-owned systems
    - the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
    - liability for loss/damage or malfunction of personal devices is clearly defined
    - there is clear advice and guidance at the point of entry for visitors to acknowledge Trust/ school requirements
    - education about the safe and responsible use of mobile devices is included in the school online safety education programmes

Social media

Our Trust and schools provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers

Trust and School staff should ensure that:

- No reference should be made in social media to learners, parents/carers or staff.
- they do not engage in online discussion on personal matters relating to members of the school communities.
- personal opinions should not be attributed to the Trust or any of the Trust schools.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

When official Trust or school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of public social media

- As part of active social media engagement, the Trust / schools may pro-actively monitor the Internet for public postings about the Trust / school.
- the Trust / school should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the Trust's complaints procedure.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The Trust / school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- the Trust / school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published.
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Trust and school procedures concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed

- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with this Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.

images will be securely stored in line with GDPR regulations .

The Trust and its schools communicate with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters
- Arbor messages/emails

The school websites are managed by school and hosted by an external provider. The Trust ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation as per the Trust's Data Protection Policy.

Cyber Security

Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach

- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage”

- the Trust has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the Trust will conduct a cyber risk assessment annually and review regularly
- the Trust, (*in partnership with their technology support partner),* has identified the most critical parts of the trust’s digital and technology services and sought assurance about their cyber security
- the Trust has an effective backup and restoration plan in place in the event of cyber attacks
- the Trust’s governance and IT policies reflect the importance of good cyber security
- staff and those in governance roles receive training on the common cyber security threats and incidents that schools experience
- the school’s education programmes include cyber awareness for learners
- the Trust has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.