

**TRINITY ACADEMY NEWCASTLE TRUST**

**Online Safety, Code of Conduct & Acceptable Use  
Policy**

**Approved by the Committee – March 2025  
On behalf of the Board**

**Next Review Date – March 2026**

**Policy Overview:**

The purpose of this policy is to safeguard and protect all members of *The Trust* online community by providing a framework to promote and maintain a safe, effective and responsive online safety culture. This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of 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).

**References:**

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

- [Teaching online safety in schools](#)
- [The Prevent Duty](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [The Prevent Duty](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

**This policy links with other policies and practices**

- *Allegation management / Whistleblowing*
- *Anti-bullying*
- *Acceptable Use Policies (AUP)*
- *Relational Behaviour Policy*
- *Child protection policy*
- *Code of conduct / staff behaviour*
- *Complaints policy*
- *Confidentiality and data protection policy*
- *Curriculum policies*
- *Data Protection*
- *Vetting Visitor Policy*

**Disclaimer**

Every effort has been made to ensure that the information contained within this policy is up to date and accurate and reflective of the latest legislative and statutory guidance. If errors are brought to our attention, we will correct them as soon as is practicable.

## 1. Online Safety Trust Statement

*The Trust asserts that online safety is an essential element of safeguarding and duly acknowledges its statutory obligation to ensure that all learners and staff are protected from potential online harm.*

*The Trust believes that the internet and associated devices are an integral part of everyday life*

*The Trust affirms that all learners should be empowered to build resilience and to develop strategies to recognise and respond to online risks.*

## 2. Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

### The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual

and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

➤ **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

#### Process for monitoring the impact of the Online Safety Policy

The Trust will monitor the impact of the policy using:

- *logs of reported incidents*
- *monitoring logs of internet activity (including sites visited using smoothwall)*
- *surveys/questionnaires of:*
  - *learners*
  - *parents and carers*
  - *staff.*

## Policy and leadership

### Responsibilities

To ensure the online safeguarding of members of our Trust community 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<sup>1</sup> and groups within the Trust.

### Governors

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

---

<sup>1</sup>

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the trust designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Michael McHugh (Chair of BOD)

All governors will:

Ensure they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

### **Head of School and senior leaders**

- The Head of School has a duty of care for ensuring the safety (including online safety) of members of the Trust community and fostering a culture of safeguarding
- The Head of School (Business) 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<sup>2</sup>.
- The Head of School (Business)/senior leaders are responsible for ensuring that the 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.
- The Head of School (Business)/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in Trust who carry out the internal online safety monitoring role.
- The Head of School (Business)/senior leaders will receive regular monitoring reports.

### **The Online Safety Lead (Trust Designated Safeguarding Lead) will:**

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined
  - take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
  - 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 Trust 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
  - receive reports of online safety incidents and create a log of incidents to inform future online safety developments
  - provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
  - liaise with (Trust/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
-

- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs

### **Academy Designated Safeguarding Lead (DSL)**

The *Academy* Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

### **Senior Leadership**

Senior Leadership will work with the Online Safety Lead to develop a planned and coordinated online safety education programme

This will be provided through:

- a discrete programme for individuals where appropriate
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#).

### **Teaching and support staff**

Trust staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current Trust 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 immediately report any suspected misuse or problem to the Academy [DSL](#) for investigation/action, in line with the Trust safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level *and only carried out using official Trust systems*

- 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 Trust activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the [SWGfL Safe Remote Learning Resource](#)
- have 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 Trust and in their use of social media.

### **Network manager/technical staff**

The network manager/technical staff is responsible for ensuring that:

- they are aware of and follow the Trust Online Safety Policy to carry out their work effectively in line with Trust policy
- the Trust 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 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 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 software/systems are implemented and regularly updated as agreed in Trust policies



## **Learners**

- are responsible for using the Trust digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this includes personal devices – where allowed)
- 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 understand the importance of adopting good online safety practice when using digital technologies out of Trust and realise that the Trust's Online Safety Policy covers their actions out of Trust, if related to their membership of the Trust.

## **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.

The Academy will take every opportunity to help parents and carers understand these issues through:

- publishing the Trust Online Safety Policy on the Trust website
- providing them with a copy of the learners' acceptable use agreement (the Trust will need to decide if they wish parents/carers to acknowledge these by signature)
- publish information about appropriate use of social media relating to posts concerning the Trust
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- 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 Trust in:*

- *reinforcing the online safety messages provided to learners in Trust*
- *the use of their children's personal devices in the Trust (where this is allowed)*

## **Community users**

Community users who access Trust systems/website/learning platform as part of the wider Trust provision will be expected to sign a community user AUA before being provided with access to Trust systems. [\(A community user's acceptable use agreement template can be found in the appendices\).](#)

*The Trust encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other Trusts and the community.*

## Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of Trust life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the Trust and wider community, using officially sanctioned Trust mechanisms.

## Policy

The Trust Online Safety Policy:

- 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 Trust and how they should use this understanding to help safeguard learners in the digital world
- describes how the Trust 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 made available to staff at induction and through normal communication channels (to be described)
- *is published on the Trust website.*

## Acceptable use

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

### Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the Trust. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- posters/notices around where technology is used

- communication with parents/carers
- built into education sessions
- Trust website

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	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:	<p><b>Any illegal activity for example:</b></p> <ul style="list-style-type: none"> <li>• Child sexual abuse imagery*</li> <li>• Child sexual abuse/exploitation/grooming</li> <li>• Terrorism</li> <li>• Encouraging or assisting suicide</li> <li>• Offences relating to sexual images i.e., revenge and extreme pornography</li> <li>• Incitement to and threats of violence</li> <li>• Hate crime</li> <li>• Public order offences - harassment and stalking</li> <li>• Drug-related offences</li> <li>• Weapons / firearms offences</li> <li>• Fraud and financial crime including money laundering</li> </ul> <p>N.B. Trusts should refer to guidance about dealing with self-generated images/sexting – <a href="#">UKSIC Responding to and managing sexting incidents</a> and <a href="#">UKCIS – Sexting in Trusts and colleges</a></p>					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> <li>• 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)</li> <li>• Gaining unauthorised access to Trust networks, data and files, through the use of computers/devices</li> <li>• Creating or propagating computer viruses or other harmful files</li> <li>• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)</li> </ul>					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	<ul style="list-style-type: none"> <li>Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>Using penetration testing equipment (without relevant permission)</li> </ul>					
Users shall not undertake activities that are not illegal but are classed as unacceptable in Trust policies:	Accessing inappropriate material/activities online in a Trust setting including pornography, gambling, drugs. (Informed by the Trust's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using Trust systems to run a private business				X	
	Using devices, systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Trust				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the Trust or brings the Trust into disrepute				X	

Consideration should be given for the following activities when undertaken for educational or non-educational purposes: Trusts may wish to add further activities to this list.	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission /awareness	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission /awareness
Non-Educational -Online gaming	x				x			
Online shopping/commerce				x	x			
File sharing		x						x

Social media			x		x			
Messaging/chat	x				x			
Entertainment streaming e.g. Netflix, Disney+	x				x			
Use of video broadcasting, e.g. YouTube,			x					x
Use of video broadcasting from social media e.g. tiktok,	x				x			
Mobile phones may be brought to Trust			x					x
Use of mobile phones for learning at Trust	x				x			
Use of mobile phones in social time at Trust			x					x
Taking photos on mobile phones				x	x			
Taking photos on cameras			x					x
Use of other personal devices, e.g. tablets, iPads, gaming devices	x				x			
Use of personal e-mail in Trust, or on Trust network/wi-fi	x				x			
Online shopping/commerce			x		x			
File sharing			x					x
AI – Non-Trust Authorised Tools	x				x		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
- 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 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., Trust website and social media. Only Trust e-mail addresses should be used to identify members of staff and learners.*

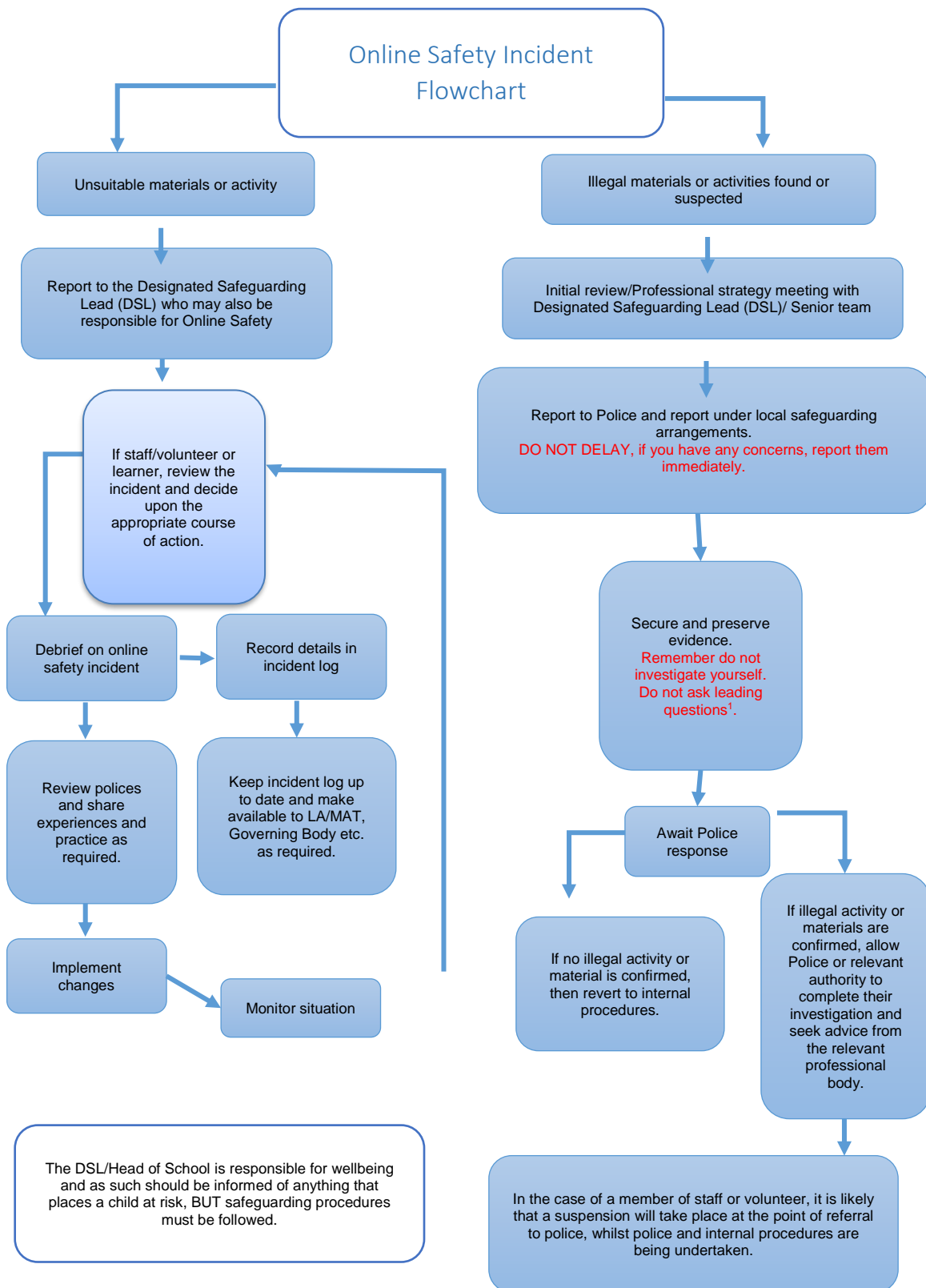
## **Reporting and responding**

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

- there are clear reporting routes which are understood and followed by all members of the Trust community which are consistent with the Trust safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the Trust 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 Trust safeguarding procedures.
- any concern about staff misuse will be reported to the Head of School, unless the concern involves the Head of School, in which case the complaint is referred to the CEO or Chair of Governors.
- 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).

- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - internal response or discipline procedures
  - involvement by local authority / MAT (as relevant)
  - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., pastoral support for those reporting or affected by an online safety incident
- incidents should be logged on Arbor
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; [Professionals Online Safety Helpline](#); [Reporting Harmful Content](#); [CEOP](#).
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  - *the ICT Focus Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
  - *staff, through regular briefings*
  - *learners, through assemblies/lessons*
  - *parents/carers, through newsletters, Trust social media, website*
  - *governors, through regular safeguarding updates*
  - *local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Trusts and Colleges suggested “working closely with Local Safeguarding Partnerships in the area where the Trust or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour”*

The Trust will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.





## Trust actions

It is more likely that the Trust 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 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

## Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Head of School	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/network/internet	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list <a href="#">in earlier section on User Actions</a> on unsuitable/inappropriate activities).		X	X	X	X	X	X	X
Attempting to access or accessing the Trust network, using another user's account (staff or learner) or allowing others to access Trust network by sharing username and passwords	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	X

Unauthorised downloading or uploading of files or use of file sharing.		X			X	X	X	X
Using proxy sites or other means to subvert the Trust'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	
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	
Unauthorised use of digital devices (including taking images)		X			X	X	X	X
Unauthorised use of online services								
Actions which could bring the Trust into disrepute or breach the integrity or the ethos of the Trust.		X		X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions.		X			X	X		X

## Responding to Staff Actions

Incidents	Refer to line manager	Refer to Head of School	Refer to HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering etc	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X	X			X
Deliberate actions to breach data protection or network security rules.		X	X		X			X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X		X	X
Using proxy sites, personal devices or other means to subvert the Trust's filtering/monitoring system.		X	X		X		X	X
Unauthorised downloading or uploading of files or file sharing		X	X		X		X	X
Breaching copyright or licensing regulations.		X	X		X		X	X
Allowing others to access Trust network by sharing username and passwords or attempting to access or accessing the		X	X		X		X	X

Trust network, using another person's account.								
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X		X	X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers		X	X		X			X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		X		X		X	X	X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		X	X		X		X	X
Actions which could compromise the staff member's professional standing		X	X		X		X	X
Actions which could bring the Trust into disrepute or breach the integrity or the ethos of the Trust.		X	X		X			X
Failing to report incidents whether caused by deliberate or accidental actions		X	X		X		X	X
Continued infringements of the above, following previous warnings or sanctions.		X	X		X			X

### Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the Trust's online safety

provision. Learners need the help and support of the Trust to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted “Review of Sexual Abuse in Trusts and Colleges” highlighted the need for:

*“a carefully sequenced RSHE curriculum, based on the Department for Education’s (DfE’s) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of ‘nudes’..”*

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be 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 matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS 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 helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside Trust*
- *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 the young people visit*
- *it is accepted that from time to time, for good educational reasons, students 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 should be 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 Trust 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 Trust community e.g. parents' evenings, family learning programmes etc.*

### Staff/volunteers

The DfE guidance "Keeping Children Safe in Education" states:

"All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."

"Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole Trust or college safeguarding approach and wider staff training and curriculum planning."

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's annual safeguarding and data protection training for all staff
- all new staff will receive cyber security training as part of their induction programme, and ensure 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) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations*
- *the Online Safety Lead will provide advice/guidance/training to individuals as required.*

## Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Academy 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/](http://www.saferinternet.org.uk/); [www.childnet.com/parents-and-carers](http://www.childnet.com/parents-and-carers) (see Appendix for further links/resources).*
- *Sharing good practice with other Trusts in clusters and MAT*

## **Governors**

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL)
- participation in Trust training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor.

## **Technology**

If the Trust has an external technology provider, it is the responsibility of the Trust to ensure that the provider carries out all the online safety and security measures that would otherwise be the responsibility of the Trust. It is also important that the technology provider is fully aware of the Trust Online Safety Policy/acceptable use agreements and the Trust has a Data Processing Agreement in place with them. The Trust should also check their local authority policies on these technical and data protection issues if the service is not provided by the authority and will need to ensure that they have completed a Data Protection Impact Assessment (DPIA) for this contract.

The Trust is responsible for ensuring that the Trust infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The Trust should ensure 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**

- the Trust filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the Trust manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre [Appropriate filtering](#). (The Trust will need to decide on the merits of external/internal provision of the filtering service – see Appendix).
- access to online content and services is managed for all users



- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC 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
  - there is a clear process in place to deal with requests for filtering changes (see Appendix for more details).
  - *the Trust has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
  - *younger learners will use child friendly/age-appropriate search engines e.g. [SWGfL Swiggle](#)*
  - filtering logs are regularly reviewed and alert the Trust to breaches of the filtering policy, which are then acted upon.
  - *where personal mobile devices have internet access through the Trust network, content is managed in ways that are consistent with Trust policy and practice.*
  - *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.* If necessary, the Trust will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site.
- 
- the Trust filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
  - the Trust manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre [Appropriate filtering.](#)
  - access to online content and services is managed for all users
  - illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC 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
  - there is a clear process in place to deal with requests for filtering changes ([see Appendix for more details](#)).
  - *the Trust has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
  - *younger learners will use child friendly/age-appropriate search engines e.g. [SWGfL Swiggle](#)*

- filtering logs are regularly reviewed and alert the Trust to breaches of the filtering policy, which are then acted upon.
- *where personal mobile devices have internet access through the Trust network, content is managed in ways that are consistent with Trust policy and practice.*
- *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.*

If necessary, the Trust will seek advice from, and report issues to, the SWGfL [Report Harmful Content](#) site.

## Monitoring

The DfE guidance “Keeping Children Safe in Education” states:

“It is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the ... risks from the Trust’s or college’s IT system. As part of this process, governing bodies and proprietors should ensure their Trust or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. “

The Trust has monitoring systems in place to protect the Trust, systems and users:

- The Trust monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- 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
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

The Trust follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance and protects users and Trust systems through the use of the appropriate blend of strategies strategy informed by the Trust’s risk assessment. [These may include:](#)

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the Trust of breaches to the filtering policy, allowing effective intervention.*

- *where possible, Trust technical staff regularly monitor and record the activity of users on the Trust technical systems*
- *use of a third-party assisted monitoring service to review monitoring logs and report issues to Trust monitoring lead(s)*

## **Technical Security**

The Trust technical systems will be managed in ways that ensure that the Trust meets recommended technical requirements

- 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
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud, (this is good practice in helping to prevent loss of data from ransomware attacks)
- all users have clearly defined access rights to Trust technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or another group)
- all users (adults 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 and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the IT Technician who will keep an up-to-date record of users and their usernames
- the master account passwords for the Trust systems are kept in a secure place, e.g. Trust safe. It is recommended that these are secured using two factor authentication for such accounts)
- passwords should be long.
- records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. *Password complexity for younger learners may be reduced (for example 6 character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged*
- password requirements for learners at Key Stage 2 and above should increase as learners progress through Trust

- The IT Technician is responsible for ensuring that all software purchased by and used by the Trust is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- appropriate security measures are in place (Trusts may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the Trust systems and data. These are tested regularly. The Trust infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.
- an agreed policy is in place (to be described) for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the Trust systems
- an agreed policy is in place (to be described) regarding the extent of personal use that users (staff / learners / community users) and their family members are allowed on Trust devices that may be used out of Trust
- an agreed policy is in place (to be described) that allows staff to/forbids staff from downloading executable files and installing programmes on Trust devices
- an agreed policy is in place (to be described) regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on Trust devices.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured. (See Trust personal data policy template in the appendix for further detail)

## **Mobile technologies**

Mobile technology devices may be Trust owned/provided and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the Trust's wireless network. The device then has access to the wider internet which may include the Trust learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile devices in a Trust context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant Trust policies including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the Trust's online safety education programme.

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

## **Social media**

The Trust 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, digital and video images policy, 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 staff should ensure that:

- no reference should be made in social media to learners, parents/carers or Trust staff
- they do not engage in online discussion on personal matters relating to members of the Trust community
- personal opinions should not be attributed to the Trust
- 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 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 Trust 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 Trust it must be made clear that the member of staff is not communicating on behalf of the Trust 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 Trust are outside the scope of this policy
- where excessive personal use of social media in Trust is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *the Trust permits reasonable and appropriate access to personal social media sites during Trust hours*

### **Monitoring of public social media**

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

Trust use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the Trust is unable to resolve support may be sought from the Professionals Online Safety Helpline.

### **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 will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- **the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.** Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education

- **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. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes**
- 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 school policies 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 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.** Permission is not required for images taken solely for internal purposes
- **parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy**
- **images will be securely stored in line with the school retention policy**
- *learners' work can only be published with the permission of the learner and parents/carers.*

## **Online Publishing**

The school communicates with parents/carers and the wider community and promotes the school through

- Public-facing website

- Social media
- Online newsletters

The school website is managed by The Trust Central Support Services. 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.

*The Trust public online publishing provides information about online safety e.g., publishing the Trust Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.*

*The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process*

## **Data Protection**

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

### **The Trust:**

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly [what personal data is held](#), where, why and which member of staff has responsibility for managing it



- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

**When personal data is stored on any mobile device or removable media the:**

- data will be encrypted, and password protected.
- device will be password protected.

- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

**Staff must ensure that they: at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse**

- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any academy personal data to personal devices.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

**Outcomes**

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the development of a consistent and effective local online safety strategy.

**9. Monitoring and Compliance**

<b>Monitoring Requirements</b>	For example: Analysing incident logs Checking planning for online safety lessons Learner, parents and carers questionnaires Evaluations
--------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------

<b>Monitoring Method</b>	Through the Self Evaluation Cycle
<b>Monitoring Prepared by</b>	Mark Kennedy –Trust Safeguarding Lead
<b>Monitoring Presented to</b>	Board of Directors
<b>Frequency of Reporting</b>	Termly

#### **10. Financial Risk Assessment**

*Consider if there are any financial risks associated with this policy*

#### **11. Consultation / Approval Process**

This policy has been devised in conjunction with the ICT Focus Group

#### **12. Dissemination and Communication Process [*\*insert locally agreed process\**]**

The policy will be placed in the Trust's Policies folder, on the Trust website and will be publicised through an induction and training update, policy update briefings for staff and notified to the Board of Directors. Newsletters and prospectus will be issued to all parents and carers.

#### **13. Development of the Policy**

This policy will be reviewed after 1 year, or earlier in the light of any incidents or investigations, legislative changes or developments in best employment practice, to ensure its continuing relevance and effectiveness.

## AUP STAFF, DIRECTORS, VOLUNTEERS, VISITORS & COMMUNITY USERS

1. (This point for staff and Directors): I have read and understood Trinity Academy Newcastle Trust's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for learners. I will report any breaches or suspicions (by adults or learner) in line with the policy without delay.
2. I understand it is my duty to support a whole-Trust safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Leads (if by a child) or Head of Trust (if by an adult).
3. **During remote learning:**
  - o **I will not behave any differently** towards learners compared to when I am in Trust. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the Trust, and will never do so directly with a learner. The same applies to any private/direct communication with a learner.
  - o **I will not attempt to use a personal system or personal login for remote teaching** or set up any system on behalf of the Trust without SLT approval.
  - o **I will not take secret recordings or screenshots** of myself or learners during live lessons.
  - o **I will conduct any video lessons in a professional environment** as if I am in Trust. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
  - o **I must always initiate the 'lobby' and invite learners and visitors in.**
  - o **I must always ensure that visitor vetting procedures are followed for all external virtual learning visitors**
  - o **I will complete the issue log for live lessons** if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of learners
4. I understand that in past and potential future remote learning there is a greater risk for grooming and exploitation as learner spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.

5. I understand the responsibilities listed for my role in the Trust's Online Safety policy. This includes promoting online safety as part of a whole Trust approach in line with the **RSHE curriculum**, as well as safeguarding considerations when supporting learners remotely.
6. I understand that Trust systems, devices and users are protected by security, monitoring and filtering services, and that my use of Trust devices, systems and logins at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
7. I understand that I must not use a personal device in school
8. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
  - not sharing other's images or details without permission
  - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the Trust community or not.
9. I will not contact or attempt to contact any learner or to access their contact details (including their usernames/handles on different platforms) in any way other than Trust-approved and Trust-monitored ways, which are detailed in the Trust's Online Safety Policy. I will report any breach of this by others or attempts by learners to do the same to the Head of School.
10. Learners Trust email addresses should not be used for sending work or for communication purposes. All communications should be made through the TEAMS platform.
11. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to Trust, I will not do it.
12. I understand the importance of upholding my online reputation, my professional reputation and that of the Academy, and I will do nothing to impair either. More guidance on this point can be found in this [Online Reputation](#) guidance for Trusts and in Trinity Academy Newcastle Trust's social media policy/guidance.
13. I agree to adhere to all provisions of the Trust Data Protection Policy at all times, whether or not I am on site or using a Trust device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and

notify the Data Manager if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.

14. I will not store Trust-related data on personal devices, USB keys, storage or cloud platforms and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
15. I will never use Trust devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
16. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the Trust. I will not browse, download or send material that is considered offensive or of an extremist nature by the Trust.
17. I understand and support the commitments made by learners, parents and fellow staff, Directors and volunteers in their Acceptable Use Policies and will report any infringements in line with Trust procedures.
18. I will follow the guidance in the safeguarding and online-safety policies for reporting incident: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handling incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
19. I understand that I am responsible for responding appropriately to Visago Alerts via the Smoothwall Filtering System whilst I work from home and from Trust
20. I understand that breach of this AUP and/or of the Trust's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the Trust and where appropriate, referral to the relevant authorities.

**To be completed by the user**

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the Trust's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

**Signature:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Role:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**To be completed by June Renwick Head of Trust (Business)** I approve this user to be allocated credentials for Trust systems as relevant to their role.

**Systems:** **TEAMS**

**Additional permissions (e.g. admin)**

**Signature:** \_\_\_\_\_

**Name:** \_\_\_\_\_

**Role:** \_\_\_\_\_

**Date:** \_\_\_\_\_

## AUP Key Stage 2

### These statements can keep me and others safe & happy at Trust and home

1. ***I learn online*** – I use the Trust's internet, devices and logons for Trustwork, homework and other activities to learn and have fun. All Trust devices and systems are monitored, including when I'm using them at home.
2. ***I learn even when I must stay at home*** – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom or nor do teachers or tutors. If I get asked or told to do anything that I would find strange in Trust, I will tell another teacher.
3. ***I ask permission*** – At home or Trust, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.
5. ***I am a friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
7. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
8. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
9. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
10. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.



- 11. I know new online friends might not be who they say they are** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
- 12. I check with a parent/carers before I meet an online friend** the first time; I never go alone.
- 13. I don't do live videos (livestreams) on my own** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
- 14. I keep my body to myself online** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
- 15. I say no online if I need to** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
- 16. I tell my parents/carers what I do online** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
- 17. I follow age rules** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult or skills but very unsuitable.
- 18. I am private online** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
- 19. I am careful what I share and protect my online reputation** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
- 20. I am a rule-follower online** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at Trust.

**21. I am not a bully** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.

**22. I am part of a community** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.

**23. I respect people's work** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.

**24. I am a researcher online** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

**25. I am not allowed to invite others to my lessons-** I must never add or invite anyone to my lessons or meetings as this keeps all my friends safe.

~~~~~

**I have read and understood this agreement.**

**If I have any questions, I will speak to a trusted adult: at Trust that includes -----**  
**-----Outside Trust, my trusted adults**  
**are** \_\_\_\_\_

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

## Acceptable Use Key Stages 3 - 5

### What am I agreeing to?

1. I will treat myself and others with respect at all times; when I am online or using any device, I will treat everyone as if I were talking to them face to face.
2. Whenever I use a device, the internet or any apps, sites and games, I will try to be positive and creative, to learn and share, to develop new skills, to have fun and prepare for the future.
3. I consider my online reputation with everything that I post or share – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
4. I will tell a trusted adult if I have a problem or am worried about something online, and I will encourage my friends to do so too. Statistics show that telling someone helps!
5. It can be hard to stop using technology sometimes, for young people and adults. When my parents/carers or teachers talk to me about this, I will be open and honest if I am struggling. I will remember the principles of the Digital 5 A Day.
6. It is not my fault if I stumble across (or somebody sends me) something violent, sexual or otherwise worrying. But I will not share or forward it, and I will ask a trusted adult for advice/help.
7. If I see anything that shows people hurting themselves or encouraging others to do so, I will report it on the app, site or game and tell a trusted adult straight away.
8. I will ensure that my online activity or use of mobile technology, in Trust or outside, will not cause my Trust, the staff, learners or others distress or bring the Trust into disrepute.
9. I will only use the Trust's internet, systems, devices and logins for Trust-related activities for activities that are appropriate to what I am doing at that time (e.g. at Trust I don't play games unless I am allowed to, e.g. during lunch, and at home I don't access inappropriate sites or apps).
10. Whenever I use the internet or devices in Trust **OR use Trust devices at home OR log in on home devices at home**, I may be monitored or filtered; the same behaviour rules always apply.
11. I will keep logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it; if I think they have used it, I will tell a teacher.

12. I will not try to bypass Trust security in any way or access any hacking files or tools.
13. I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
14. I will use the internet, apps, sites & games responsibly; I will not use any that are inappropriate for Trust use or for my age, including sites which encourage hate or discrimination.
15. I understand that any information I see online could be biased and misleading, so I should always check sources before sharing (see [fakenews.lgfl.net](https://fakenews.lgfl.net) for support).
16. I understand that bullying online or using technology is just as unacceptable as any other type of bullying, and will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at Trust or outside. I will stand up for my friends and not be a bystander.
17. I will not post, look at, up/download or share material that could be offensive, harmful or illegal. If I come across any, I will report it immediately.
18. I know some sites, games and apps have age restrictions (most social media are 13+) and I should respect this. 18-rated games are not more difficult but inappropriate for young people.
19. When I am at Trust, I will only message or mail people if it's relevant to my learning.
20. Messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the Trust.
21. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will not open a file, hyperlink or any other attachment.
22. I will not download copyright-protected material (text, music, video etc.).
23. I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
24. Livestreaming can be fun, but I always check my privacy settings and know who can see what and when. If I livestream, my parents/carers know about it.
25. I know new online friends might not be who they say they are, so I am always very careful when someone wants to 'friend' me. Unless I have met them face to face, I can't be sure who they are.

26. I will never arrange to meet someone face to face who I have only previously met in an app, site or game without telling and taking a trusted adult with me.
- 27. When learning remotely, teachers and tutors will not behave any differently** to when we are in Trust. If I get asked or told anything that I would find strange in Trust, I will tell another teacher.
28. I must never add or invite anyone else to a lesson or meeting online. This is the teachers job.
29. I will only use my personal devices (mobiles, smartwatches etc) in Trust if I have been given permission, and I will never take secret photos, videos or recordings of teachers or learners, **including when learning remotely.**
30. I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting photos or videos that show me or anyone else without all my/their clothes on.
31. Many apps can identify where I am or where I made a post or took a photo, so I know how to turn off location settings so everyone doesn't see where I am, where I live or go to Trust.
32. What I do on devices should never upset or hurt others & I shouldn't put myself or others at risk.
33. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, sexual, extremist/hateful content, I will not respond to it but I will talk to a trusted adult about it.
34. I don't have to keep a secret or do a dare or challenge just because someone (even a friend) tells me to – real friends don't put you under pressure to do things you don't want to.
35. It is illegal to view any form of pornography if you are under 18 years old; I will not attempt to do so and will report anyone who tries to trick me into doing so.
36. I can always say no online, end a chat or block someone; if I do, it's best to talk to someone, too.
37. I know who my trusted adults are at Trust, home and elsewhere, but if I know I can also get in touch with Childline, The Mix, or The Samaritans.

~~~~~

**I have read and understand these rules and agree to them.**

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

## Acceptable Use for Parent/Carers

### What am I agreeing to?

1. I understand that Trinity Academy Newcastle Trust uses technology as part of the daily life of the Trust when it is appropriate to support teaching & learning and the smooth running of the Trust, and to help prepare the learners and young people in our care for their future lives.
2. I understand that the Trust takes every reasonable precaution to keep learners safe and to prevent learners from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the Trust cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in Trust, and use of Trust-owned devices, networks and cloud platforms out of Trust may be subject to filtering and monitoring. These should be used in the same manner as when in Trust, **including during any remote learning periods.**
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the Trust staff, volunteers, Directors, contractors, learners or other parents/carers.
5. The impact of social media use is often felt strongly in Trusts, which is why we expect certain behaviours from learners when using social media. I will support the Trust's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the Trust's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's learner on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The Trust sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
7. I understand that for my child to grow up safe online, s/he will need positive input from Trust and home, so I will talk to my child about online safety.
8. **I understand that my child needs a safe and appropriate place to do remote learning if Trust or bubbles are closed (similar to regular online homework). When on any video calls with Trust, it would be better not to be in a bedroom but where this is unavoidable, my child will be fully dressed and not in bed, and the camera angle will point away from**

**beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.**

- 9. If my child has online tuition for catchup after lockdown or in general, I will undertake necessary checks where I have arranged this privately to ensure they are registered/safe and reliable, and for any tuition remain in the room where possible, and ensure my child knows that tutors should not arrange new sessions or online chats directly with them.**
10. I understand that whilst home networks are much less secure than Trust ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. [swiggle.org.uk](http://swiggle.org.uk) and YouTube Kids is an alternative to YouTube with age appropriate content.
11. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my learners, and refer to the principles of the Digital 5 A Day: [learnerscommissioner.gov.uk/our-work/digital/5-a-day/](http://learnerscommissioner.gov.uk/our-work/digital/5-a-day/)
12. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
13. I can find out more about online safety at Trinity Academy Newcastle Trust by reading the full Online Safety Policy and can talk to the Designated Safeguarding Lead form tutor, class teacher, etc ] if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in Trust.

~~~~~

**I/we have read, understood and agreed to this policy.**

**Signature/s:**

\_\_\_\_\_

**Name/s of parent / guardian:**

\_\_\_\_\_

**Parent / guardian of:**

\_\_\_\_\_

**Date:**

\_\_\_\_\_

Support for Learners to keep them safe online

- [Calm Zone](#) – activities to help let go of stress
- [games](#) to help take your mind off things
- [information and advice](#) on a range of topics including feelings, relationships, family and Trusts
- peer support [message boards](#)
- [Childline Kids](#), our website for under 12s.

Childline can also give confidential help and advice. Calls to 0800 1111 are free or learner can [get support online](#).

Support for Parents and carers to keep their learner safe online

Use these resources to support parents and carers to keep their learner safe online:

- [Thinkuknow](#) provides advice from the National Crime Agency (NCA) on staying safe online
- [Parent info](#) is a collaboration between Parentzone and the NCA providing support and guidance for parents from leading experts and organisations
- [Childnet](#) offers a toolkit to support parents and carers of learner of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- [Internet matters](#) provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help learner get the most out of their digital world
- [London Grid for Learning](#) has support for parents and carers to keep their learner safe online, including tips to keep primary aged learner safe online
- [Net-aware](#) has support for parents and carers from the NSPCC, including a guide to social networks, apps and games
- [Let's Talk About It](#) has advice for parents and carers to keep learner safe from online radicalisation

For Education Staff : UKCIS [guidance](#) on sharing nudes and semi-nudes



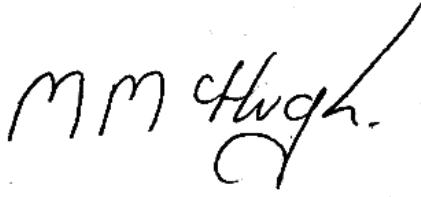
## Appendix 4: online safety training needs – self audit for staff

| ONLINE SAFETY TRAINING NEEDS AUDIT                                                                        |                                    |
|-----------------------------------------------------------------------------------------------------------|------------------------------------|
| Name of staff member/volunteer:                                                                           | Date:                              |
| Question                                                                                                  | Yes/No (add comments if necessary) |
| Do you know the name of the person who has lead responsibility for online safety in Trust?                |                                    |
| Are you aware of the ways learners can abuse their peers online?                                          |                                    |
| Do you know what you must do if a learner approaches you with a concern or issue?                         |                                    |
| Are you familiar with the Trust's acceptable use agreement for staff, volunteers, Directors and visitors? |                                    |
| Are you familiar with the Trust's acceptable use agreement for learners and parents?                      |                                    |
| Do you regularly change your password for accessing the Trust's ICT systems?                              |                                    |
| Are you familiar with the Trust's approach to tackling cyber-bullying?                                    |                                    |
| Are there any areas of online safety in which you would like training/further training?                   |                                    |

**Signed** .....

**Date**.....

**Signed on behalf of Board of Directors:**

A handwritten signature in black ink, appearing to read "MM Hugh". The signature is written in a cursive, stylized font. The first two letters "MM" are large and prominent, followed by the word "Hugh" in a more fluid script. A long, sweeping horizontal line extends from the end of the signature.

---

**Michael McHugh (Chairperson for the Board)**

**Date: March 2025**