FIERTÉ
MULTI-ACADEMY TRUST
Proudly inspiring all to excellence

Caring • Individuality • Bravery • No one left behind

Online Safety Policy

Document and Version Control

Document Title	Online Safety Policy
Effective Date	1st September 2025
Policy Owner	Safeguarding Forum
Policy Approver	Trust Board

Version	Date	Amended by	Comments
4.0	18th January 2023	Linda Webster and Ryan Byrne	Policy re-draft as part of Trust IT policy overhaul.
4.1	27th June 2024	Ryan Byrne	Annual review.

Section	Changes Made

Contents

Online Safety Policy 1
Document and Version Control 2
Introduction 4
Rationale 4
Scope 4
Roles and Responsibilities 5
Academy Leadership 5
Trust Leadership 5
Teaching and Support Staff 5
Learners 6
Parents and Carers 6
Education 6
Learners 6
Parents 7
The Wider Community 7
Staff and Volunteers 8
Preventative Technical Measures 8
Acceptable Use 9
Agreements 9
Images and Videos 9
Social Media 9
Cyberbullying 10
Responding to Misuse 10
Classifying Usage 10
Managing Online Safety Incidents 10
Appendix 1 12
Appendix 2 14
Appendix 3 1

Introduction

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any individual and it helps to promote equality across Fierté Multi-Academy Trust.

Rationale

The Trust recognise the vast opportunities offered to children and young people through digital technologies and the potential educational benefits for learning. However, such technologies can also pose significant threats to children's safety, development and wellbeing.

Online platforms are not consistently policed. All users need to be aware of the risks associated and constraints including minimum age requirements (*in most cases, 13 years old*).

The Trust understand our responsibility to educate learners in online safety issues; teaching appropriate behaviours and critical thinking skills. Young people must be empowered to remain safe and legal when using digital technologies beyond just the classroom context.

This policy aims to:

- Identify responsibilities for stakeholders relating to learner's online safety.
- Specify expected, acceptable usage and behaviour of learners.
- Highlight avenues for staff, parent / carer and community online safety education.
- Ensure a consistent, comprehensive approach to online safety across the Trust.

This policy should be read alongside the Acceptable Use Agreements.

Scope

Online safety applies where devices and applications can connect or communicate with others. The Trust identify that children and young people may be using many such technologies both inside and outside of the classroom. This may include:

Tablets, Desktops and Laptops	**Mobile Telephones**	**Web Browsing**	**Virtual Learning Environments**	**Social Media**
Email	**Blogs**	**Online Gaming**	**Instant Messaging**	**Chat Rooms**
Online Research	**Podcasts**	**Live Streaming**	**Smart TVs**	**Video Sharing**

It is important to recognise the continuous, fast-paced evolution of digital technologies within society at large. This policy will be monitored and regularly evaluated taking into considering any incidents which may have occurred or wider technological developments. Where appropriate, the policy will be adapted to ensure it remains relevant and up to date.

Roles and Responsibilities

Academy Leadership

Each academy has identified a member of staff as the IT Curriculum Lead. This individual holds day to day responsibility for online safety in their academy. As part of this role, they must ensure staff are aware of procedures that need to be followed in the event of an online safety incident. They provide advice and training for staff to ensure online safety is embedded in all aspects of the curriculum.

All designated safeguarding members of staff should be suitably trained in online safety issues and should be aware of the potential for serious child protection / safeguarding issues to arise.

Online safety is an important aspect of strategic leadership within our Trust. As such, the Headteacher and Governors of each academy have ultimate responsibility to ensure that relevant policies and practices are both embedded and monitored.

Trust Leadership

Where appropriate, the Trust will ensure that IT Managed Service Providers (MSPs) are aware of our online safety policies and procedures. The Trust Technical Manager (TTM) will work alongside academy IT Curriculum Leads providing support for and advice on the safe use of technologies.

It is important to emphasise that online safety incidents are primarily safeguarding issues and not necessarily technical issues. However, technological solutions can empower staff and help to minimise or detect the development of such issues.

The Chief Executive Officer holds strategic responsibility for safeguarding across the Trust. Strategic responsibility for IT remains with the Trust Vice-CEO to whom the TTM reports.

Teaching and Support Staff

All staff across the Trust are expected to:

- Have an up-to-date awareness of online safety matters and current online safety policies and practices.
- Have read, understood and signed an Acceptable Use Agreement.
- Embed online safety issues in the curriculum.

- Pre-check websites and resources as suitable before directing learners during lessons where internet use is planned.
- Follow processes in place for dealing with unsuitable material found.

Learners

All learners are responsible for using technology in accordance with the Learner Acceptable Use Agreement. Learners should also:

- Have a good understanding of online research skills.
- Understand the need to avoid plagiarism or copyright infringement.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Understand the importance of adopting good online safety practice when using digital technologies inside and out of school.

Parents and Carers

Parents and carers play a crucial role in ensuring children understand the need to use digital technologies in an appropriate way. They must sign the Learner Acceptable Use Agreement on behalf of their child/ren and explain this in an age-appropriate manner.

Education

Learners

The education of learners in online safety and digital literacy is essential. Children and young people need the help and support of our academies to recognise and manage online safety risks while building their resilience.

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:

- As part of Computing, PSHE and other lessons - regularly revisited.
- Key online safety messages as part of a planned programme of assemblies through learning and PSHE activities.
- Learners taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Learners taught to acknowledge the source of information used and respect copyright when using material accessed on the internet.

- Learners supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Learners helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the academy.
- Staff 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 are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material. Where pupils are allowed to freely browse the internet, staff must be vigilant in monitoring the content of the websites visited.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in sites being blocked. In such a situation, staff may request that the Trust Technical Team make temporarily exception for specific sites during the period of study. Any request to do so should be auditable – submit via the Support Portal – with clear reasons for the need. Additional authorisation from the academy's SLT may be required before proceeding.

Parents

Parents and carers may only have a limited understanding of online safety risks and issues. They may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure of how to respond.

Academies will seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters and academy websites
- Parents / Carers evenings and sessions
- High profile events and campaigns such as Safer Internet Day
- Reference to relevant websites and publications such as:
  - South West Grid for Learning (SWGfL.org.uk)
  - UK Safer Internet Centre (SaferInternet.org.uk)
  - Childnet (Childnet.com)

The Wider Community

The Trust may provide opportunities for local community groups or members of the community to gain from academies' online safety knowledge and experience. This may be offered through the following:

- The Trust / academy websites.
- Providing family learning courses in use of new technologies, digital literacy and online safety.

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- Supporting community groups such as Early Years settings, childminders, youth / sports / voluntary groups to enhance their online safety provision.

Staff and Volunteers

It is essential that all staff / volunteers receive online safety training and understand their responsibilities, as outlined in this policy. Academies are responsible for providing a tailored programme of online safety training for all staff.

Continued professional development may be offered through:

- Attendance at external training events.
- Sharing of guidance released by relevant bodies and Trust staff.
- Presentations and discussion opportunities in staff / team meetings and INSET days.

As part of their induction programme, all new staff and volunteers should ensure they understand the Trust Online Safety Policy **and** relevant Acceptable Use Agreements. When updates are made to such documents, this should be shared via academies' internal communication routes.

Guests will be issued with an Abridged Internet Safety Policy also asked to sign an Acceptable Use Agreement as part of the Supply Staff pack.

Preventative Technical Measures

The Trust is responsible for ensuring that academies' infrastructure and networks are as safe and secure as reasonably possible. In collaboration with Managed Service Providers, the Trust will ensure that academy infrastructure meets statutory requirements. The Trust will achieve this through cyber security arrangements identified in the Trust Cyber Security Policy.

While onsite, users of Trust IT resources can expect DNS-based web filtering (*likely managed by an external service provider*). Differentiated, user-level filtering policies allow variation in the experience for groups of users (*such as staff and learners*) when using domain-joined devices. Content lists are regularly updated and, where technically possible, usage is logged.

The Trust's filtering and monitoring should ensure that children are safe from illegal and extremist material when accessing the internet. However, no technical solution can accurately detect and restrict **all** such content. Consequently, academies must immediately report any sites which appear to circumvent these measures.

As described in the Trust Cyber Security policy, the Technical Manager and Technical Team can only manage compliance of systems and devices on which they have been appropriately consulted on and provided sufficient access. In executing their responsibilities, they are reliant upon information supplied by others within academies. For example, during installation of new filtering systems, restricted and permitted categories are agreed first by headteachers.

Acceptable Use

Agreements

The primary purpose of technology in an academy context is educational and must be consistent with relevant policies. This includes, but is not limited to, academies' safeguarding, anti-bullying and behaviour policies.

Teaching about the safe and appropriate use of mobile technologies should be an integral part of academies' online safety curriculum.

Amongst others, the Trust has produced the following concise, age-appropriate Acceptable Use Agreements:

EYFS and KS1 Class Agreement	KS2 Class Agreement	Learner Agreement

The Trust expect that:

- Class agreements are discussed with learners during the transition period or at the start of each new academic year.
- Academy Senior Leadership and Offices ensure parents / carers review and sign a learner agreement on behalf of their child/ren.

Images and Videos

Images and videos may remain available on the internet forever. This can cause harm or embarrassment in the short and longer time. Academies will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.
For example:

- When using digital media, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution. In particular, they should recognise the risks attached to publishing their own images / videos on the internet such as on social networking sites.
- Written permission will be obtained from parents or carers before photographs or videos of pupils are published on the Trust / academy websites, social media pages or in the local press.

Social Media

The Trust has a duty of care to provide a safe learning environment for pupils and staff. Schools, academies, Trusts and local authorities could be held responsible indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may

render the academy or Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place. Please refer to the Trust Social Media Policy for further information.

Cyberbullying

Cyberbullying is the use of IT, most commonly mobile phones and the internet, to deliberately upset someone else. The whole Trust community has a duty to protect all its members and provide a safe, healthy environment.

The Educations and Inspections Act 2006 states that Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils when they are off site. It is important that we work in partnership with pupils and parents / carers to educate them about cyberbullying as part of online safety.

They should:

- Understand how to use these technologies safely and know about the risks and consequences of misusing them.
- Know what to do if they or someone they know are being cyber bullied.
- Report problems with cyberbullying. If they do have a problem, they can talk to the academy, parents/carers, the police and platform providers to do something about it.

Responding to Misuse

Classifying Usage

Some digital activities could lead to criminal prosecution. There are however a range of activities which may be legal but would be inappropriate in the academy context - either because of the age of the users or the nature of those activities. The Trust identifies examples of usage in Appendix 1.

Managing Online Safety Incidents

There may be times when a user's actions are in violation of this policy and/or the Acceptable Use Agreements. This may take place through careless, irresponsible or deliberate misuse.

The flow chart provided in Appendix 2 provides guidance for staff responding to online safety incidents. It is intended to encourage a safe and secure approach to the management of the incident. Upon suspicion of illegal activity, staff should refer to the right-hand side of the flowchart and report immediately to the police.

Upon suspicion of misuse or inappropriate content, all steps in this procedure should be followed:

- Involve more than one senior member of staff in the process to protect individuals if accusations are subsequently made.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. 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 or print screenshots of the content from the machine being used for investigation **except in the case of images of child sexual abuse**.
- Once the incident has been investigated, the group will need to judge whether this concern has substance or not. If it does, the incident must be dealt with as soon as possible in a proportionate manner. The appropriate action may include:
    - An internal response following behavioural consequence / disciplinary procedures.
    - Involvement of the Trust Board or national / local organisations as relevant.
    - Involvement of the Police.
- If incident being reviewed includes images of child abuse, the **monitoring should be halted immediately and referred to the Police**. Other cases to report to the police would include:
    - Incidents of 'grooming' behaviour.
    - The sending of obscene materials to a child.
    - Adult material which potentially breaches the Obscene Publications Act.
    - Criminally racist material.
    - Promotion of terrorism or extremism.
    - Other criminal conduct, activity or materials.
- If necessary, isolate the device in question as best you can. Any change to its state may hinder a later police investigation.

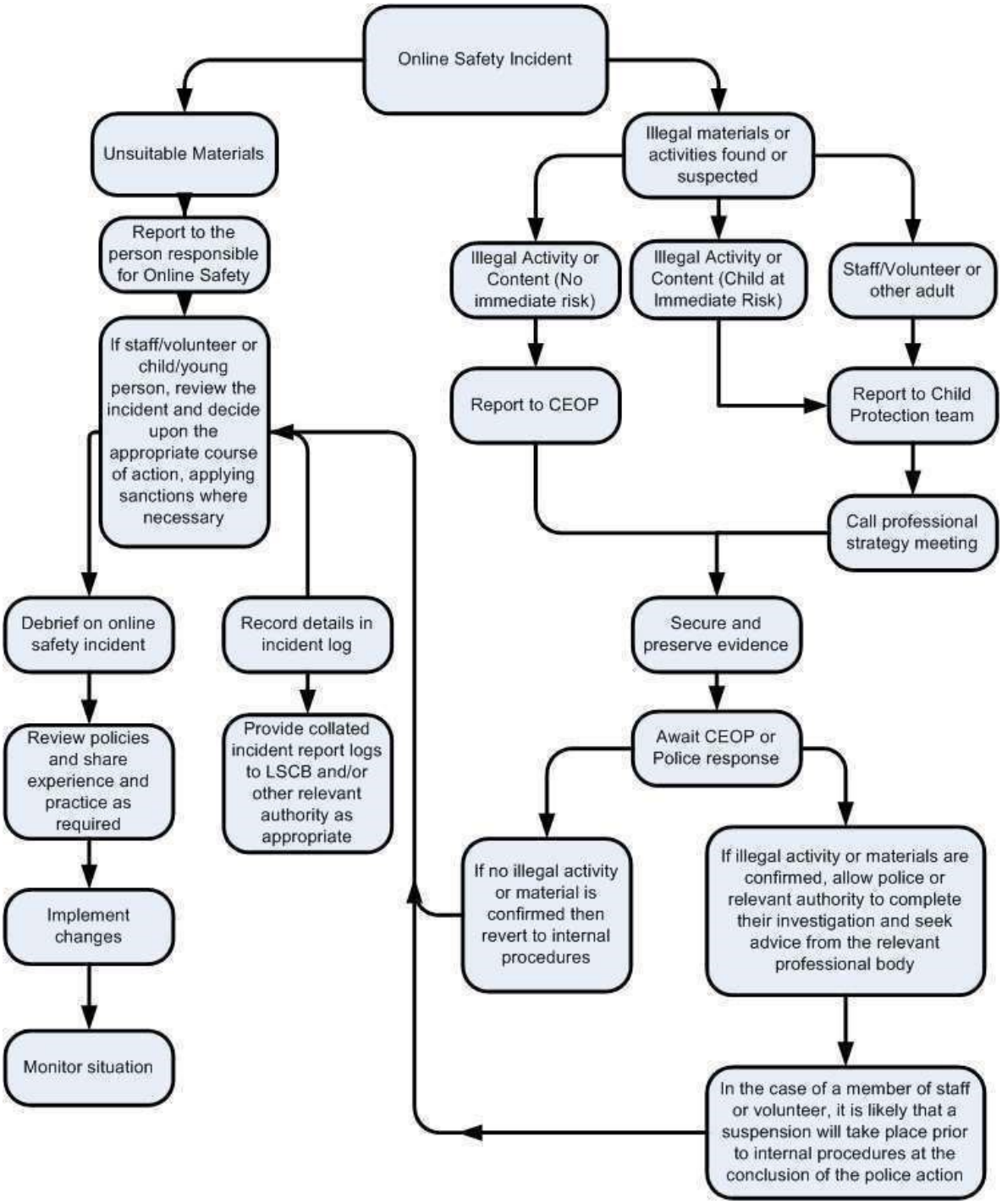
It is important that all the above steps are taken to provide an evidence trail and to demonstrate that visits to these sites were carried out for safeguarding purposes. An example proforma for recording incidents and action taken is provided in Appendix 3. However, academies may choose to use a different form / recording system. Completed records should be retained by the group for evidence and reference purposes.

Appendix 1

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit sites, make, post, download, upload, transfer, communicate or otherwise share material, remarks, proposals or comments that contain or relate to:	Child sexual images – The making, production or distribution of indecent images of Children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character). Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation). Contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Trust or brings the Trust into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg: financial / personal information, databases, access codes or passwords)					X	
Creating or propagating computer viruses or other harmful files.					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

Educational online games	X				
Online gambling				X	
Online shopping / commerce		X			
File sharing	X				
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting		X			

Appendix 2


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix 3

Example Online Safety Incident Record

Date	Time	Incident Description	Action Taken		Recorded By	Signature
			What?	By Whom?		