

Document Title	Online Safety Policy
Author/Owner (Name and Title)	ICT Support
Version Number	V1
Date Approved	27 July 2026
Approved By	Board of Trustees

Policy Category (Please Indicate)	1	Trust/Academies to use without amendment
	2	Academy specific appendices
	3	Academy personalisation required (in highlighted fields)

Summary of Changes from Previous Version

Version	Date	Author	Note/Summary of Revisions
V1	June 2026	Exec	New Policy

TABLE OF CONTENTS

1. STATEMENT OF INTENT	3
2. SCOPE	3
3. LEGAL FRAMEWORK	3
4. ONLINE SAFETY RISK FRAMEWORK	4
5. ROLES AND RESPONSIBILITIES	5
6. MANAGING ONLINE SAFETY	6
7. VULNERABLE LEARNERS	8
8. REPORTING AND RESPONDING TO CONCERNS	8
9. ICT ACCEPTABLE USE	9
10. MONITORING AND REVIEW	9
APPENDIX A	9
APPENDIX B.....	11

1. STATEMENT OF INTENT

The Trust is committed to safeguarding and promoting the welfare of children through the safe, secure and responsible use of technology.

Online safety is a core component of safeguarding. The Trust recognises that risks to children arise both online and offline, and that digital platforms, systems and services form part of the safeguarding environment.

This policy defines how the Trust manages online safety through:

- Education.
- Technical controls.
- Age-appropriate access.
- Monitoring and intervention.

2. SCOPE

This policy applies to:

- All students.
- Staff, governors and volunteers.
- Contractors, visitors and third parties.
- Use of technology both on and off Trust sites where it impacts safeguarding.

It includes:

- Internet-enabled platforms and services.
- Social media and online communication.
- Artificial intelligence tools.
- Filtering and monitoring systems.

3. LEGAL FRAMEWORK

This policy operates within the following statutory, regulatory and organisational framework.

LEGISLATION

This policy is underpinned by the relevant UK legislation and statutory guidance:

- Keeping Children Safe in Education (KCSIE) – 2026.
- Online Safety Act 2023.
- Children's Wellbeing and Schools Act 2026.
- Data Protection Act 2018 / UK GDPR.
- Counter-Terrorism and Security Act 2015 (Prevent Duty).

The Online Safety Act places legal duties on platforms to:

- Prevent illegal content.

- Protect children from harm.
- Implement effective age assurance.
- Assess and reduce risk.

LINKED DOCUMENTS

This policy will be implemented in accordance with the following Trust policies and procedures:

- Safeguarding Policy.
- ICT Acceptable Use Policy.
- Behaviour Policy.
- Artificial Intelligence Use Policy.
- Staff Code of Conduct Policy.

4. ONLINE SAFETY RISK FRAMEWORK

The Trust recognises four categories of online risk:

- Content – exposure to harmful or illegal material.
- Contact – harmful interaction with others.
- Conduct – unsafe behaviour and misuse.
- Commerce – scams, fraud and financial risk.

Emerging risks include:

- Cyberflashing and image-based abuse.
- Encouragement of self-harm.
- AI-generated harm and deepfakes.

5. ROLES AND RESPONSIBILITIES

TRUST BOARD

- Provides oversight of safeguarding and online safety.
- Ensures compliance with statutory requirements.

PRINCIPALS / LEADERS

- Ensure effective implementation of this policy.
- Ensure appropriate filtering, monitoring and safeguarding controls.

DESIGNATED SAFEGUARDING LEAD (DSL)

- Leads online safety across the Academy.
- Oversees filtering and monitoring effectiveness.
- Ensures all concerns are reported, recorded and acted upon.
- Reviews trends and informs improvement.

ICT SUPPORT

- Implements and maintains technical safeguards.
- Ensures systems are secure and appropriately configured.
- Supports safeguarding investigations.

ALL STAFF

- Model safe and professional online behaviour.
- Identify and report concerns.
- Support students to use technology safely.

STUDENTS

- Use technology responsibly.
- Follow Acceptable Use expectations.
- Report concerns and seek help.

6. MANAGING ONLINE SAFETY

EDUCATION

Students receive an age-appropriate online safety curriculum aligned to UKCIS “Education for a Connected World”.

This framework describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.

Categories include:

1. Self-image and identity.
2. Online relationships.
3. Online reputation.
4. Online bullying.
5. Managing online information.
6. Health, wellbeing, and lifestyle.
7. Privacy and Security.
8. Copyright and ownership.

The use of external support where appropriate, will complement education approaches.

SOCIAL MEDIA PLATFORM RISK AND AGE-APPROPRIATE ACCESS

The Trust recognises that:

- Social media platforms present differing levels of risk.
- National policy is moving towards restricting access for younger users.

The Trust promotes:

- Age-appropriate access to platforms.
- Awareness of platform-specific risks.
- Safe and supported progression into digital environments.
- Recognition that platform access itself is increasingly a safeguarding control.

AGE ASSURANCE AND VERIFICATION

Online services are required to implement increasingly robust age assurance controls as part of safeguarding under UK law.

The Trust recognises:

- These controls are an important safeguarding measure.
- Risks exist where controls are bypassed or manipulated.

Students are supported to understand:

Reviewed: June 2026

- Why age restrictions exist.
- Risks of sharing personal or biometric data.
- Consequences of circumventing safeguards.

TECHNICAL CONTROLS

Filtering and monitoring systems form a core part of the Trust's safeguarding arrangements and are subject to oversight, review and assurance.

- Academy DSL's takes lead responsibility for safeguarding and child protection including online safety and the filtering and monitoring systems in place.
- ICT Support are responsible for maintaining Internet filtering solutions across the Academy/Trust.

Filtering

The Trust operates filtering systems that prevent access to illegal, inappropriate and potentially harmful content. Filtering is applied by default to all users and devices accessing Trust networks and internet services. The Trust ensures that filtering arrangements support safeguarding responsibilities under KCSIE, the Prevent Duty, the Online Safety Act, and the DfE Filtering and Monitoring Standards

- Access is filtered to block harmful or inappropriate content (Appendix B).
- Controls are age-appropriate and regularly reviewed.
- Staff may request sites to be blocked based on inappropriate content. This should be reported to ICT Support through the service desk, who will action immediately.
- There may be occasions where websites are unnecessarily blocked. Staff may request a website be unblocked by submitting a request to ICT Support via the service desk. DSL's will check the site and unblock if appropriate.
- Filtering applies to all trust owned and managed devices.

Monitoring

- Activity is monitored as part of safeguarding.
- Alerts identify potential risk.
- Safeguarding staff review and respond to reports and alerts.

ARTIFICIAL INTELLIGENCE (AI)

AI introduces new safeguarding risks, including:

- Misinformation and manipulation.
- Exploitation and impersonation.
- Generation of harmful or inappropriate content.

The Trust's 'Policy on the use of Artificial Intelligence' outlines Place Partnership's vision and strategy regarding the implementation of AI tools, how we fulfil our obligation to comply with safeguarding and data protection legislation, and promote the understanding and ethical use of AI among all stakeholders

Concerns relating to AI are treated as safeguarding concerns where appropriate.

7. VULNERABLE LEARNERS

Some students may be more vulnerable to online harm.

The Trust will ensure:

- Targeted education.
- Increased monitoring where appropriate.
- Appropriate safeguarding support.

8. REPORTING AND RESPONDING TO CONCERNS

STUDENTS

Students are encouraged to report any concerns regarding their online safety to a member of the Safeguarding team or indeed, any trusted adult.

- Concerns can also be reported via an online form found in the Safeguarding section of each Academies website.
- Academy websites list links to several external agencies that offer a variety of advice and support.

INCIDENTS INVOLVING STUDENTS

All online safety concerns must be reported and recorded in line with safeguarding procedures.

- Incidents relating to child protection are dealt with by the DSL in accordance with academy and Local Authority procedures. This type of incident could include for example:
 - Online sexual violence and sexual harassment – non-consensual sharing of sexual images and video, sexualised online bullying, unwanted sexual comments on social media.
 - Sharing of nudes/semi-nudes (also known as youth produced sexual imagery).
 - Online radicalisation and extremism.
- Incidents of cyberbullying are dealt with in accordance with the Academy/Trust Anti-Bullying and Behaviour policies.
- If you do not want to approach the user or are unsure of the seriousness of the incident, you should report it to a senior member of staff who will progress the matter as appropriate.
- If you witness or are informed of anyone acting inappropriately, you should politely remind them of this Online Safety policy and of the ICT Acceptable Use Agreement (AUA) to which they have agreed.

INCIDENTS INVOLVING STAFF

- Incidents involving staff should be reported to the Academy Principal or Chief Executive Officer.
- Appropriate action will then be taken in line with Child Protection and Safeguarding procedures.

9. ICT ACCEPTABLE USE

- This policy defines safeguarding expectations.
- User behaviour, system use, and rules are defined within the ICT Acceptable Use Policy.

10. MONITORING AND REVIEW

The Trust will:

- Review online safety arrangements regularly.
- Monitor incidents and trends.
- Benchmark against recognised frameworks.
- Update policy in line with legal and technological developments.

APPENDIX A - CONTACTS

ACADEMY CONTACTS

Refer to each Academies Child Protection and Safeguarding Policy.

LOCAL AUTHORITY

Rotherham - Multi Agency Safeguarding Hub	(MASH)	01709 336080
Doncaster Council Children's Services		01302 737777
Barnsley – Multi Agency Safeguarding Hub	(MASH)	01226 772423
Wakefield – Multi Agency Safeguarding Hub	(MASH)	03458 503503

EXTERNAL

South/West Yorkshire Police	999 Emergency 101 non-Emergency
------------------------------------	------------------------------------

Meeting Digital & Technology Standards in Schools & Colleges – Filtering & Monitoring
<https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard>

Child Exploitation and Online Protection Centre	(CEOP)	0207 979 5835 http://ceop.police.uk
--	--------	--

Childline	0800 1111 http://www.childline.org.uk
------------------	--

Childnet – Advice for parents and carers.	https://www.childnet.com/parents-and-carers
--	---

Digizen - Information for educators, parents, carers, and young people.	http://www.digizen.org
--	---

NSPCC – Keeping safe online.	https://www.nspcc.org.uk/keeping-children-safe/online-safety
-------------------------------------	---

Internet Matters – Online safety guidance and support	https://www.internetmatters.org
--	---

UK Safer Internet Centre	https://swgfl.org.uk/projects/uk-safer-internet-centre
---------------------------------	---

Wakefield Safeguarding Children Partnership	https://wakefieldscp.org.uk/
--	---

APPENDIX B – INTERNET FILTER CATEGORIES

Categories blocked by default

MANDATORY ILLEGAL CONTENT

The following categories are always be blocked and cannot be disabled:

- Child Sexual Abuse Material (CSAM).
- Terrorist and extremist material.
- Content promoting or facilitating terrorism.
- Content promoting violent extremism or radicalisation.
- Illegal drugs and drug supply.
- Illegal weapons sales.
- Fraud and criminal activity.
- People smuggling and illegal immigration facilitation.
- Content promoting or facilitating suicide.
- Intimate image abuse and illegal sexual content.
- Coercive and controlling behaviour content where illegal.
- Incitement to violence or hate crime content.

PLACE PARTNERSHIP ALSO SPECIFICALLY FILTER:

Prevent Duty Related Content

- Extremist ideology.
- Terrorist propaganda.
- Radicalisation content.
- Recruitment material from proscribed organisations.
- Hate-based extremist content.
- Violent political or religious extremism.

Harmful and Inappropriate Content

- Pornography and sexually explicit material.
- Adult dating services.
- Gambling.
- Violence and gore.
- Self-harm promotion.
- Eating disorder promotion.
- Abusive or hateful content.
- Racist or discriminatory material.
- Bullying and harassment sites.
- Dangerous challenges and stunt content.
- Promotion of substance misuse.
- Violence Against Women and Girls (VAWG) content.
- Content normalising abuse or misogyny [smoothwall.com], [saferinternet.org.uk]

Technical Circumvention Tools

- VPN services.
- Anonymous proxies.
- Tor and anonymising services.
- Filter bypass tools.
- Unauthorised remote desktop services.

Emerging Online Risks

- Harmful AI-generated content.
- Generative AI systems that are not approved by the school.
- Misinformation and disinformation.
- Conspiracy theory content that could cause harm or radicalisation.