Fulwood academy

Online Safety Policy

We Care • We Challenge • We Commit

Document Control Table			
Document Title:	Online Safety Policy		
Owner:	Dunstone Education Trust		
Approved on:			
Author Name:	PER		
Version	1		
Approved by:	Dunstone Trust Board		
Review date:	September 2026		
Document History:			
Version	**Date**	**Author**	**Note of revisions**
V1	Sept 24	PER	Adoption of the Policy

Table of Contents

Fulwood Academy Online Safety Policy Mission Statement

At Fulwood Academy, we are committed to fostering a safe, responsible, and respectful digital environment for all members of our school community. Guided by our core values—**We Care, We Challenge, We Commit**—we ensure that online safety remains a priority in our learning and social interactions.

- **We Care** by promoting a culture of respect, kindness, and digital well-being, ensuring that every student feels safe and supported online.
- **We Challenge** by empowering students to think critically, recognise online risks, and develop the skills needed to navigate the digital world responsibly.
- **We Commit** to maintaining a secure online environment through education, clear policies, and collaborative efforts with students, staff, and parents to uphold the highest standards of digital safety.
  Together, we strive to create a positive and secure digital space where everyone can learn, grow, and thrive with confidence.

1. Introduction

Fulwood Academy is committed to ensuring that all members of the school community are safe online. This policy outlines our approach to educating students, protecting staff and learners, and maintaining a secure digital environment through robust filtering, monitoring, and online safety education.

This policy aligns with:

- ✓ Fulwood Academy's Safeguarding and Child Protection Policy (2024-2025)
- ✓ Acceptable Use Agreement
- ✓ DfE Filtering and Monitoring Guidance (2023)
- ✓ Keeping Children Safe in Education (KCSIE) 2024
- ✓ UKCIS 'Education for a Connected World' Framework

2. Roles and Responsibilities

2.1 Leadership & Governance

The Principal and Governing Body ensure:

- Online safety remains a priority within safeguarding strategies.
- Regular policy reviews take place to maintain compliance with DfE expectations.
- The school provides appropriate online safety training for staff and students.

2.2 Designated Safeguarding Lead (DSL) & Online Safety Lead

The DSL is responsible for:

- Overseeing the implementation of online safety measures, including filtering and monitoring systems.
- Responding to online safety incidents and reporting concerns where necessary.
- Liaising with external agencies (e.g., police, local safeguarding teams) when serious online risks arise.

2.3 IT Team

The IT Team ensures:

- The school's filtering and monitoring systems comply with DfE guidance.
- Regular checks and audits are conducted on digital security measures.
- Any attempts to bypass school filters or security measures are investigated and reported on the filtering and monitoring tracker.

2.4 Teaching & Support Staff

- Embed online safety education into lessons and school activities.
- Encourage students to report online concerns.
- Understand their responsibilities in relation to filtering and monitoring.

2.5 Students

- Follow the Acceptable Use Agreement when using school technology.
- Report any online risks or concerns via My Voice, peer mentors, or trusted staff.
- Engage in online safety education programmes.

2.6 Parents & Carers

- Support school efforts in monitoring and safeguarding students online at home.
- Actively read and engage with school communications around online safety.

3. Education & Awareness

3.1 Online Safety Curriculum

Online safety is integrated into PSHE, RSHE, Computing, and pastoral sessions, following the UKCIS 'Education for a Connected World' framework, covering:

- Cyberbullying & Online Abuse
- Online Grooming & Exploitation
- Misinformation & Fake News
- Data Privacy & Digital Footprints
- Social Media Safety & Emerging Technology Risks
- AI generated content and deepfakes
- Live streaming risk
- Online Radicalisation

3.2 Staff Training & Professional Development

- Annual online safety training for all staff, including specialised training for DSLs and IT teams.
- Training includes identifying online threats, understanding digital trends, and safeguarding SEND students online.
- Annual cyber security training for all staff specialising in education cyber awareness.

3.3 Parent & Community Engagement

- Termly online safety updates for parents
- Guidance on home filtering and parental controls provided via newsletters and school communications.
- External sources of help e.g saferinternet.org.uk or NSPCC
- Parental interactive workshops on evolving online risks

4.0 Artificial Intelligence (AI)

4.1 Use of AI in an Educational Context

The school acknowledges the potential benefits of AI in education, including:

- Enhancing teaching and learning.
- Improving learning outcomes.
- Supporting administrative processes and reducing staff workload.
- Preparing learners for a future where AI will be an integral part of society and the workforce.

Staff are encouraged to use AI-based tools to support their work where appropriate, within the frameworks provided below. Staff must act professionally and be accountable for their use of AI.

4.2 AI and Compliance with Safeguarding & Data Protection

- The school will comply with all relevant legislation and guidance, including Keeping Children Safe in

Education and UK GDPR.

- Training will be provided for staff and governors on the advantages, use, and risks of AI.
- The school will support staff in identifying training and development needs to enable relevant opportunities.
- The curriculum will integrate learning about AI, ensuring that students understand:
- How AI works.
- Its potential benefits, risks, and ethical implications.
- Social and economic impacts of AI.

4.3 Responsible AI Use for Staff

- Staff, Parents and Pupils will be supported in using AI tools responsibly, ensuring the protection of personal and sensitive data.
- Only anonymised data may be inputted into AI tools to avoid exposure of personally identifiable information.
- AI tools must comply with UK GDPR and data protection regulations.
- Staff must only use school-provided AI accounts for work purposes to ensure compliance with security and oversight requirements.
- Sensitive data must not be inputted into third-party AI tools unless they have been vetted and approved for this purpose.

4.4 Ethical Use of AI & Transparency

- AI tools must not infringe copyright or intellectual property. Care must be taken to ensure that learner-created content is not used to train AI models without consent.
- AI-generated content in documents, emails, presentations, or teaching materials must be clearly labelled to maintain transparency and trust.
- Staff must verify AI-generated content for accuracy before sharing or publishing to prevent the spread of misinformation.
- AI should assist, not replace, human decision-making. Final judgments must always be made by a person.

4.5 AI Risk Assessment & Incident Management

- Any AI-related incidents, data breaches, or misuse must be reported immediately to the school's safeguarding or IT team.
- The school will audit all AI systems in use, assessing their impact on staff, learners, and school procedures.
- AI tools will be monitored for potential discrimination or bias in outputs, with interventions in place to mitigate risks.
- Improper use of AI (including breaches of data protection) may result in disciplinary action in line with the school's Staff Disciplinary Policy.

4.6 AI and Parental Engagement

- The school will support parents and carers in understanding the use of AI in education through an "AI in Our School Guide".
- Parents will be informed of how AI is used in school settings and any implications for their child's learning and safety.
- A version of this guide is available for pupils.

5.0 Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant access to images for educational use. However, staff, parents/carers, and students must be aware

of the risks associated with publishing digital images on the internet, including:

- The potential for online bullying or misuse of images.
- Digital images remaining accessible online indefinitely, which may cause harm or embarrassment in the future.
- Employers conducting internet searches on potential and existing employees, including reviewing publicly available digital content.

To mitigate risks, Fulwood Academy will:

- Educate students and staff on the risks of digital imagery use, including the taking, sharing, and publishing of images.
- Ensure images of students who cannot be photographed are only taken on school-approved devices, not personal staff devices.
- Allow parents/carers to take digital images at school events for personal use only, with a reminder not to share images publicly or on social media.
- Permit staff and volunteers to take digital/video images to support educational activities, in compliance with school policies on storage and sharing.
- Ensure students are appropriately dressed in all shared digital images.
- Prohibit students from taking or sharing images of others without explicit permission.
- Only publish photographs of students that have been carefully selected and in compliance with the Online Safety Policy.
- Ensure that students' full names are not used in online publications alongside photographs.
- Obtain written parental/carer consent before using student images on the school website or social media (see Acceptable Use Agreement).
- Inform parents/carers of the intended use, storage, and duration of images, in accordance with the school's Data Protection Policy.
- Securely store images in line with the school's retention policy.
- Only publish student work with explicit learner and parental consent.
- Report any accounts to POSH (Professionals Online Safety Helpline) that may be slanderous towards any professional body in school or maliciously using school owned materials I.E Fulwood Academy Badge/Dunstone Education Trust Logo.

6.0 Social Media

With the widespread use of social media for professional and personal purposes, Fulwood Academy recognises the need for clear guidance to help manage risks and ensure responsible online behaviour.

The school takes reasonable steps to protect learners, staff, and the school community by:

- Ensuring that personal information is not published.
- Providing education and training on acceptable use, age restrictions, social media risks, privacy settings, and reporting issues.
- Establishing clear reporting procedures for inappropriate use.
- Conducting risk assessments, including legal risks associated with social media.
- Offering guidance for learners and parents/carers on responsible social media use.

6.1 Staff Responsibilities on Social Media

School staff should:

- Not reference learners, parents, or staff on personal social media.
- Avoid engaging in online discussions relating to school matters.
- Ensure that personal opinions are not attributed to the school.
- Regularly check privacy settings to minimise the risk of data exposure.

- Act as positive role models in their use of social media.

6.2 Official School Social Media Accounts

When using social media for school purposes:

- All accounts must be approved by senior leadership.
- There must be clear processes for moderation, behaviour expectations, and reporting concerns.
- Any abuse or misuse of school social media accounts will be investigated and addressed under the school's disciplinary procedures.

6.3 Personal Use of Social Media

- If a staff member's personal social media account references or impacts the school, they must include a disclaimer stating they are not speaking on behalf of the school.
- Excessive personal social media use during school hours may result in disciplinary action.
- Staff are permitted reasonable and appropriate access to personal social media during break times.

6.4 Monitoring of Public Social Media

The school proactively monitors public social media for references to the school. When concerns arise on social media, the school will:

- Encourage direct communication to resolve issues privately.
- Direct parents/carers to the school's complaints procedure if concerns remain unresolved.

The Online Safety Lead and senior leadership regularly review the school's social media presence.

6.3 Process for Addressing Social Media Issues Outside of School

Social media incidents that occur outside of school hours and off school grounds. The school's primary responsibility is to maintain a safe and supportive learning environment, but it does not regulate or intervene in personal social media interactions that occur outside of school.

1. **Clarification of School's Role**

- The school is not responsible for monitoring or addressing social media activity that occurs outside of school hours and off school premises.
- Parents and guardians are encouraged to monitor their child's online activity and address concerns directly.

2. **Reporting Concerns**

- If a student or parent reports a social media issue that occurred outside of school, they will be advised to handle it privately or seek assistance from appropriate authorities (e.g., parents, social media platforms, or law enforcement if necessary).
- If the issue directly impacts the school environment (e.g., threats of violence, bullying that continues in school), it may be reviewed under the school's behaviour policies.

3. **Guidance for Students and Parents**

- Students will be encouraged to use social media responsibly and respectfully.
- Parents/guardians will be advised to discuss internet safety and responsible social media use with their children.
- If necessary, families may be directed to online safety resources or law enforcement if the concern involves legal matters (e.g., harassment, threats, or illegal activity).

4. Exceptions

- If a social media issue outside of school directly affects school safety, disrupts learning, or violates school policies, the school may take action in accordance with its behaviour code.

7.0 Mobile Technologies

7.1 Overview

Mobile technology devices may be school-owned or personally owned and include smartphones, tablets, laptops, wearable devices, and any other internet-connected technology. These devices may access the school's wireless network, learning platforms, and cloud-based services, requiring clear guidelines to protect students, staff, and the school community.

All users must understand that the primary purpose of mobile and personal device use in a school context is educational. The school's mobile technology policy is aligned with other policies, including safeguarding, behaviour, anti-bullying, acceptable use, and IT security.

All devices within the school environment—whether school-owned, BYOD (Bring Your Own Device), or guest-owned—will be subject to our firewall and filtering systems. This ensures that every user is appropriately filtered and monitored in accordance with the school's ICT Acceptable Usage Policy and Safeguarding Policies.

7.2 School-Owned/Provided Devices

The school has the following measures in place for mobile devices provided by the school:

- Devices are managed through Mobile Device Management (MDM) software or on premise central management to ensure security and compliance.
- An asset log is maintained detailing who each device is allocated to.
- Clear guidelines specify where, when, and how school-owned devices can be used.
- Personal use (e.g., online banking, shopping, personal images) is regulated and communicated clearly.
- The use of school devices on trips or events is defined with clear expectations.
- Liability for damage aligns with the school's policy on equipment replacement.
- Students receive education on the responsible use of school-provided mobile devices.
- Filtering and monitoring on school previsioned devices ensure that each individual that will access and or use a device will be correctly filtered within the user groups that is assigned to them I.E all students will be filtered under the pupil polices which has greater restrictions than staff.

7.3 Personal Devices

There is a clear policy for the use of personal mobile devices on school premises for all users.

- Where devices are used to support learning, staff receive training to ensure equitable access to required resources for all students.
- The use of personal devices for school business is defined in the Acceptable Use Policy and Staff Handbook.
- Personal devices connected to the school network are segregated from school-owned systems to maintain security.
- The use of personal devices for taking, storing, or sharing images/videos must align with the school's Acceptable Use Policy and Digital & Video Images Policy.
- The non-consensual taking or use of images of others is strictly prohibited.
- Liability for loss, damage, or malfunction of personal devices is clearly defined in the school policy.
- Visitors receive clear guidance on mobile device use upon entry to the school.
- Online safety education includes guidance on the safe and responsible use of mobile devices.

- Staff personnel personal devices will under go the same filtering and monitoring as they would while on a school device. However, fewer restrictions will apply to allow certain material normally blocked I.E Social media.
- Guest Devices are filtered heavily to prevent potential cyber risks and inappropriate content within school – this is acknowledged in the inventory sign in system.
- Any users that connect a personally owned device within school agree that all network and search content is actively monitored and will be subject to our schools' policies.

7.4 Risks of Mobile & Smart Technology

The DfE guidance Keeping Children Safe in Education states that:

"Schools should recognise that many children have unrestricted access to the internet via mobile phone networks (3G, 4G, and 5G), and should include this in their mobile and smart technology policy and child protection policy."

Mobile and smart technology presents risks such as:

- Online sexual harassment, bullying, and exploitation via messaging apps and social media.
- The use of encrypted messaging apps (e.g., WhatsApp, Telegram) for unsafe or unsupervised communication.
- Accessing harmful or inappropriate content through unrestricted mobile data networks.

To address these risks, the school:

- Educates students about **safe mobile technology use and digital wellbeing**.
- Implements **robust filtering and monitoring policies** for school-owned devices.
- Encourages parental involvement in **monitoring and managing children's mobile device use outside of school**.

8.0 . Filtering & Monitoring

Fulwood Academy ensures compliance with the DfE Filtering and Monitoring Guidance, maintaining a safe online environment for all users.

8.1 Filtering (Prevention of Harmful Content)

The school uses SOPHOS firewall and filtering software to block access to inappropriate or harmful content, including:

- Extremism and radicalisation material
- Self-harm or suicide content
- Online pornography or explicit content
- Cyberbullying platforms and forums
- Filtering systems are customised for different user groups (e.g., stricter restrictions for younger students).
- The IT team and DSL conduct termly reviews to update filtering settings as digital risks evolve.

8.2 Monitoring (Detection of Online Risks)

- SOPHOS firewall and filtering monitoring software is used to track and flag potentially unsafe online activity.
- Students and staff are made aware of what is being monitored and why (briefing and Monday Key Messages).
- The DSL and IT team receive automated alerts when a student searches for concerning topics (e.g., self-harm, violence, exploitation).

- Keyword tracking and behavioural monitoring help detect early warning signs of digital risks.
- All incidents flagged by monitoring software are reviewed, logged, and escalated appropriately.
- All staff have access to a system called AB Tutor which allows them to see pupil screens and monitor keywords and activity during a computer lesson.
- The IT Team and DSL has access to a system called netsupport DNA which shows a breakdown of different keywords and issues I.E Selfharm, Radicalization etc.

8.3 Response to Filtering & Monitoring Alerts

- Immediate review of alerts by the DSL & IT Team.
- Incidents involving safeguarding concerns (e.g., attempted access to extremist content, grooming risks) are reported to external safeguarding agencies.
- Disciplinary action is taken where students attempt to bypass security measures or engage in harmful online behaviour.

8.4 Transparency & Review of Filtering & Monitoring Policies

- Filtering and monitoring settings are reviewed daily to ensure they are effective and proportionate.
- Students and staff are made aware of what is being monitored and why.
- Reports on filtering effectiveness are shared with the leadership team and governors to ensure accountability.

9.0 Reporting & Incident Management

9.1 Student Reporting Channels

Students can report concerns via:

- My Voice anonymous reporting system
- A trusted member of staff
- Peer mentors/Digital Leaders

9.2 Staff Reporting Responsibilities

- All online safety incidents must be immediately reported to the DSL via the school's safeguarding system.
- Staff can also report incidents connected to them via the Professionals Online Safety Helpline (POSH) (For example and social media post about them or an account intimating them)

9.3 Response to Online Safety Incidents

Investigation & Action Plan:

DSL reviews all reported incidents. Disciplinary Action: If a student breaches the Acceptable Use Agreement, appropriate sanctions are applied. Sanctions can include:

- IMPACT
- Suspensions
- Exclusion
- Network ban
- External Referral: Serious concerns (e.g., online grooming, radicalisation risks) are escalated to external safeguarding agencies.

Levels of Breach and Consequences

Low-Level Breach (e.g., minor filter bypass attempts, one-time violations)

- IMPACT: Verbal warning and reminder of the Acceptable Use Agreement.
- Parental Involvement: Parents/carers will be informed of the violation.
- Restriction: Temporary loss of internet privileges (e.g., one-week network restriction).

Medium-Level Breach (e.g., repeated filter bypass attempts, accessing inappropriate but non-dangerous material)
IMPACT: Formal warning recorded in school behaviour logs.

- Parental Involvement: Meeting with parents/carers to discuss concerns.
- Restriction: Extended internet ban (e.g., one month) and restricted access to personal devices during school hours.
- Monitoring: Additional monitoring of student's online activities.

High-Level Breach (e.g., deliberate circumvention of security measures, sharing bypass methods, accessing harmful content)

- IMPACT: Disciplinary action in line with school behaviour policy.
- Parental Involvement: Formal meeting with parents/carers and written warning.
- Restriction: Long-term or permanent network and internet access ban.
- Suspension: Possible suspension depending on severity and intent.
- Police Involvement: If laws have been broken (e.g., accessing illegal content, cyber threats, or online harassment), the incident will be reported to the police.

Severe Breach (e.g., engaging in illegal online activities, distributing harmful material, hacking school systems)
-

- Parental Involvement: Urgent meeting with parents/carers and external safeguarding agencies.
  Restriction:
- IMPACT: Immediate and severe disciplinary action, up to and including permanent exclusion.
- Permanent ban on using school digital resources.
- Suspension/Exclusion: Depending on the severity of the offence.
- Police Involvement: The school will report serious breaches to law enforcement and cooperate with investigations.

10.0. Student Involvement in Online Safety

- Students participate in Safer Internet Day, digital citizenship projects, and peer-led awareness campaigns.
- Peer mentoring groups support younger students in understanding digital risks and responsible online behaviour.
- Digital Leaders assist in reviewing school policies and providing feedback on filtering and monitoring practices.

11.0. Policy Review & Compliance

- This policy is reviewed annually by the DSL, IT Team, and Leadership.
- The filtering and monitoring systems are assessed termly to maintain compliance with DfE standards.
- Staff, students, and parents are consulted to ensure the effectiveness of online safety measures.