John Taylor Free School

Online Safety Procedure

This procedure should be read in conjunction with the JTMAT Online Safety Statement and the JTFS Safeguarding Procedure.

Author	Mrs L Bosworth
Implementation Date:	January 2022
Reviewed:	September 2024, March 2026
Next Review due:	September 2026

JTFS Online Safety Guidance

1. Aims

John Taylor Free School (JTFS) is committed to providing a safe digital environment for all members of the school community. In accordance with our safeguarding framework, our core objectives are:

- Robust Processes: Maintaining rigorous procedures to ensure the online safety of students, staff, volunteers, and governors through persistent monitoring and policy enforcement.
- Community Empowerment: Delivering a proactive approach to online safety that protects and educates the whole school community—including visitors—on the safe and ethical use of technology.
- Clear Intervention Mechanisms: Establishing definitive, "if-this-then-that" protocols to identify, intervene in, and escalate online incidents effectively.
- Whole-School Protection: Implementing comprehensive safeguarding mechanisms to protect every individual within the community, ensuring digital infrastructure supports rather than hinders student welfare.

2. Legislation and Guidance

This document is constructed in alignment with the following statutory and non-statutory frameworks:

- Keeping Children Safe in Education (KCSIE) 2025.
- Online Safety Act 2023.
- Data Use and Access Act 2025.
- Data Protection Act 2018 and UK GDPR.
- Education Act 1996 and 2011.
- Equality Act 2010.
- Education and Inspections Act 2006.
- Voyeurism (Offences) Act 2019.

3. Roles and Responsibilities

Local Governing Body

The Governing Board provides strategic leadership and is responsible for:

- Ensuring the Designated Safeguarding Lead (DSL) remit explicitly covers online safety.
- Monitoring the effectiveness of filtering and monitoring systems (at least annually) in liaison with ICT staff.
- Ensuring all governors receive appropriate online safety training at induction and regular intervals to provide strategic challenge.

Headteacher

- The Headteacher ensures consistent implementation of this guidance and supports the DSL by providing the necessary time, resources, and funding to maintain a robust digital safety infrastructure.

Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety, including:

- Logging and managing online safety incidents via the school's formal reporting procedure.
- Providing half-termly data reports on online safety to the Governing Body.
- Liaising with external agencies, including the police and children's social care, as required.
- Disseminating safety information via Safeguarding E-Newsletters to staff. Senior IT Technician

Senior IT Technician

The Senior IT Technician manages the technical infrastructure and is responsible for:

- Updating filtering and monitoring systems to protect users from harmful content, including extremist material.
- Conducting full monthly security checks on all ICT systems.
- Vetting and whitelisting of Generative AI tools in accordance with DfE safety standards.

All Staff

All staff, including contractors and volunteers, must:

- Model professional online conduct and ensure students adhere to Acceptable Use Agreements (AUA).
- Maintain professional curiosity to identify children who may benefit from Family Help.
- Report concerns immediately via the established school reporting procedures. Parents & Students

Students: Must adhere to the AUA, report concerning online experiences, and seek assistance if they encounter inappropriate content.

Parents: Are expected to monitor home online activity, promote digital safety, and use social media appropriately regarding the school.

Visitors and Members of the Community: Visitors, including contractors and community members using the school's ICT systems or internet, are bound by the same AUA standards as staff and students. Failure to comply may result in the withdrawal of access and referral to safeguarding leads.

4. Educating Students

Online safety is integrated into the curriculum to provide age-appropriate education:

- Key Stage 3: Focuses on protecting online identity and privacy, recognizing inappropriate content/conduct, and reporting procedures.
- Key Stages 4 and 5: Addresses how technological changes (including AI) affect safety, advanced privacy protection, and the legalities of social media use.
- Delivery: Utilizes timetabled lessons, assemblies, and pastoral provision to address "teachable moments," such as emerging hoaxes or online challenges.

5. Educating Parents

The school maintains a partnership with parents to ensure digital safety extends beyond the school gates:

- Reporting: If parents have queries or concerns regarding online safety, they should raise these in the first instance with the Safeguarding Team.
- Communication: Regular updates are shared via letters, newsletters, and the school website.
- Resources: Parents are encouraged to consult:
    - UK Safer Internet Centre: Issue-specific advice.
    - Childnet: Factsheets and "hot topics."
    - CEOP: Reporting and guidance on exploitation.

6. Cyber-bullying

Cyber-bullying is the repetitive, intentional harming of an individual or group online involving an imbalance of power.

1. Prevention: The school actively discusses cyber-bullying in registration and assemblies to explain consequences and reporting methods.
2. Search and Deletion: Under the Education Act 2011, staff have the legal power to search for and delete inappropriate files or images on a student's device where there is a "good reason." A "good reason" is established when staff reasonably suspect the file has been, or could be, used to:
    - Cause harm
    - Disrupt teaching
    - Break school rules

7. Self-Generated Intimate Images

When responding to concerns regarding self-generated intimate images, the school follows strict safeguarding protocols:

1. Staff MUST NOT: Under any circumstances, ask to view or see the images or videos.
2. Immediate Action: Report the concern to the DSL or Deputy DSLs immediately.
3. Safeguarding Response:
4. Speak to the child involved and involve parents/carers.
5. Determine the DfE classification of the image.
6. Assess the need for a referral to the police or social services.

7. Supervise the deletion of the content and signpost the student to ChildLine for additional support.

8. Acceptable Use (Filtering and Monitoring)

The JTFS technical monitoring stack provides proactive, real-time protection across the network All Windows devices (both student and staff) have Smoothwall Monitor installed which provides proactive real-time monitoring.

- The client captures user activity as it happens and automatically sends potential risks through to the Monitor portal and the safeguarding team are alerted instantly to any potential high-risk alerts.
- Our Sophos Web Filtering allows us to have separate Staff and Student Filtering policies, therefore ensuring that suitable filtering levels are applied per user.
- Sophos provides dynamic categorization, therefore ensuring that all new websites are categorized appropriately.

Entrust Monitoring Service protects students from harmful content. It is a granular, content aware filtering service that reviews, monitors and tracks and notifies us of any safeguarding risks including radicalisation, suicide and self-harm.

Alert Protocol: Immediate email alerts for high-risk ("Grade 4/5") captures are sent to the assigned leads:

1. Laura Bosworth – Designated Safeguarding Lead
2. Michelle Hassell - Deputy DSL "Graded Captures" trigger an immediate investigation, location identification, and pastoral follow-up.

9. Mobile and Smart Technology

- Personal Devices: Not permitted for student use during school hours without explicit permission. The school assumes no responsibility for these devices.
- School Devices: Loaned devices are managed via Mobile Device Management (MDM) software and are subject to the same filtering and monitoring standards as the internal network.
- Staff Use: Personal devices must not be used during lesson time (except in emergencies) or used to photograph students.

10. Generative AI

In compliance with 2026 DfE safety standards, Generative AI use is managed as follows:

1. Product Filtering: Only AI tools with built-in safety filters vetted by the Senior IT Technician are permitted.
2. Cognitive Offloading: Monitoring ensures AI does not replace critical thinking or skill development.
3. Anthropomorphisation: Staff and students are educated to avoid treating AI agents as sentient or human-like.

4. Data Privacy: Entry of personal, sensitive, or identifiable data into Large Language Models (LLMs) is strictly forbidden.
5. Age Restrictions: All use must comply with provider-set age limits.

11. Response to Misuse

- Students: Misuse is handled via the Behaviour Procedure. Grade 4/5 captures trigger mandatory parental notification and investigation.
- Staff: Misuse is handled via Disciplinary Procedures.
- Legal Action: Any activity involving illegal content will be reported to the police without delay.

12. Training

- Induction: All new staff receive training on safe internet use, cyber-bullying, and radicalization.
- Annual Updates: All staff receive annual safeguarding refreshers, including filtering and monitoring responsibilities.
- Specialist Training: The DSL and deputies undertake specialist training every two years, with annual knowledge updates to stay abreast of requirements.

13. Monitoring Arrangements

This guidance is a "live" document reviewed annually by the DSL.
Review results and anonymised incident logs are shared with the Governing Board to ensure the policy reflects current technological risks and statutory changes.

14. Links with Other Policies

This document should be read alongside:

- JTFS Safeguarding Procedure
- Behaviour Procedures
- Staff Code of Conduct
- Data Protection Policy
- JTMAT Online Safety Statement
- ICT Security - Acceptable Use Policy
- JTMAT AI Policy
- Comments, Compliments and Complaints procedure