TAKE 1 STUDIOS

Online Safety Policy

CREATED	**September 2026**
CREATED BY	**Naomi Fearon**
NEXT REVIEW DATE	**September 2027**

1. Summary

The E-Safety Policy ensures that children, young people, and staff are able to use the internet and related technologies safely and responsibly. It is part of our wider safeguarding duty of care and aligns with the Take 1 Whole School Safeguarding Policy. This policy equips staff, students, and parents/carers to identify, prevent, and respond to online risks effectively.

Keeping Children Safe in Education (KCSIE 2025) places a duty on schools to ensure that technology use is safe, productive, and free from harm. As technology evolves, schools must remain vigilant in protecting young people from risks such as online grooming, child sexual exploitation (CSE), sexting, image-based abuse, radicalisation, bullying, and AI-generated content such as deepfakes. The DSL has overall responsibility for promoting online safety and ensuring that robust systems are in place to safeguard all members of the school community.

2. Purpose of this Policy

The purpose of this Online Safety Policy is to:
- Define clear principles for safe and responsible use of technology by all members of the Take 1 community.

- Safeguard and protect students, staff, and the wider school community online.
- Raise awareness of both the risks and benefits of technology.
- Establish clear procedures for reporting and responding to online safety concerns.
- Ensure compliance with KCSIE 2025 and other statutory guidance, including filtering and monitoring requirements.
- Support staff, students, and parents/carers to develop digital resilience.

3. Scope

This policy applies to:

- All staff, governors, volunteers, contractors, and visitors to Take 1.
- All students, parents, and carers.
- Any individual or organisation using the school's network, equipment, or digital platforms.

4. Filtering and Monitoring (KCSIE 2025)

The school must have effective filtering and monitoring systems in place to prevent access to harmful online content, including extremist material, pornography, self-harm websites, and online exploitation platforms.

Our filtering and monitoring systems will:

- Be reviewed annually and updated regularly to address emerging threats.
- Include AI-powered monitoring to detect harmful patterns such as grooming, radicalisation, and bullying.
- Be tested and audited by both technical staff and the governing body to ensure effectiveness.
- Provide weekly logs to the DSL and Head Teacher for review.
- Include procedures to escalate breaches immediately via CPOMS.

The governing body is responsible for ensuring the effectiveness of these systems and will receive termly reports on filtering and monitoring activity.

5. Roles and Responsibilities

Designated Safeguarding Lead (DSL): Naomi Fearon (Head Teacher)

- Oversees implementation of this policy.
- Ensures all staff and students understand online safety procedures.
- Provides training and updates on emerging risks, including AI-related harms.
- Liaises with external agencies such as CEOP, MASH, and the Police where appropriate.

Deputy DSLs: Courtney Rose, Roshell McFarlane, Shannon Berrington

- Support the DSL and lead on online safety incidents as required.

Technical Lead: Courtney Rose

- Maintains network security and filtering systems.
- Ensures secure authentication for all users.
- Conducts regular system reviews and reports breaches immediately.

Safeguarding Governor: Theo Harris
- Ensures compliance and oversight at a governance level.
- Receives termly reports on incidents and filtering/monitoring audits.

6. Training and Awareness

- All staff receive annual safeguarding and online safety training, including current trends such as live streaming, AI content, and online radicalisation.
- Governors receive online safety training at least every three years.
- Pupils receive age-appropriate education on digital literacy and safe online practices.
- Parents are provided with workshops and resources to support safe technology use at home.

7. Reporting and Incident Management

All online safety concerns must be reported to the DSL and recorded via CPOMS. The following process will be followed:
1. Immediate safeguarding risk assessed by DSL.
2. Serious incidents reported to CEOP or the Police.
3. Parents/carers informed where appropriate, unless doing so places a child at greater risk.
4. Records kept securely and reviewed for patterns of concern.

Any data breaches will be reported following the Take 1 Data Protection and Cyber Security Policy and GDPR requirements.

8. Emerging Risks

We recognise that new risks emerge as technology evolves. This includes:

- AI-generated content and deepfakes.
- Online financial exploitation and scams targeting young people.
- Harms associated with live streaming and gaming platforms.
- Risks from smart devices, wearables, and IoT-enabled technology.

The DSL will review these risks annually and ensure appropriate responses are embedded into school practice.

9. Related Policies

This policy must be read alongside:

- Take 1 Whole School Safeguarding Policy.
- Anti-Bullying Policy.
- Behaviour Policy.
- Acceptable Use Policies.
- Photographic Image Use Policy.
- Data Protection and Cyber Security Policy.

10. Review and Governance

The E-Safety Policy will be reviewed annually by the DSL and approved by the governing body. Interim reviews will take place if significant safeguarding concerns arise or new statutory guidance is issued.