# TAO E-Safety Policy

## Ethos Statement

**TAO Independent School** recognises that Information and Communication Technology (ICT), including internet-based tools and mobile devices, is a vital part of modern life. Our commitment is to ensure that all young people, particularly those with SEND and trauma histories, are safeguarded from potential online harms, while being equipped with digital literacy and resilience to safely navigate technology.

### Purpose

This policy applies to all members of the TAO community including staff, pupils, parents/carers, volunteers, and visitors. It covers the use of all digital technologies within and outside of the provision including devices, internet platforms, mobile phones, social media, gaming systems, and any emerging technology.

This policy aligns with current statutory guidance, including Keeping Children Safe in Education 2026, the Prevent Duty, the Data Protection Act 2018, UK GDPR, and the Education (Independent School Standards) Regulations 2014 (as amended). This policy should be read in conjunction with the Safeguarding & Child Protection Policy, Behaviour Management Policy, Mobile Phone & Smart Device Policy, Staff Code of Conduct, Acceptable Use Agreement, Prevent Policy, and Data Protection & Privacy Policy.

### Principles

- The Headteacher, as Designated Safeguarding Lead, holds safeguarding oversight of online safety arrangements.
- Technical implementation and review of filtering and monitoring systems is supported by the IT Support Provider / Nominated IT Lead. Safeguarding oversight remains with the Designated Safeguarding Lead.
- All staff receive online safety information and safeguarding updates as part of induction and ongoing safeguarding training. Additional online safety training is provided according to role, responsibility and identified need
- Students are taught safe, respectful, and responsible online behaviours across the curriculum.

## Digital Safety in the Curriculum

E-Safety education is reinforced across the curriculum and in staff CPD, ensuring all adults model safe, responsible, and ethical digital use in line with the TAO Code of Conduct

E-Safety is embedded throughout curriculum delivery and our SMSC provision. Topics include:

- Cyberbullying awareness.
- Online grooming and radicalisation.
- Data privacy and password protection.
- Appropriate use of social media.
- Respectful digital communication.
- Understanding misinformation and digital footprints. Online safety education also includes age-appropriate teaching about generative AI, AI chatbots, deepfakes, image manipulation, nudification tools, synthetic media, online coercion, image-based abuse, and the risks associated with sharing personal or intimate images.
- Pupils are taught to understand that online content may be manipulated, misleading, extremist, abusive or generated by artificial intelligence, and are supported to develop critical thinking and safe reporting behaviours.
-

## Inclusive and Trauma-Informed Practice

TAO is committed to supporting learners with SEND and trauma through accessible digital education:

- E-Safety content is delivered with visual aids, clear language, and appropriate scaffolding.
- Sessions include discussions about emotional regulation when online.
- Risk reduction strategies are co-developed with students and parents/carers.

## Acceptable Use and Incident Reporting

Any online safety concern which may involve harm, abuse, exploitation, grooming, radicalisation, inappropriate sexual content, image-based abuse or other safeguarding risk must be reported immediately to the DSL or DDSL and recorded in accordance with the Safeguarding & Child Protection Policy. Technical breaches or systems concerns must also be reported to the IT Support Provider / Nominated IT Lead where appropriate

## Safe Use of Email, Devices, and Mobile Phones

- Staff use TAO-issued email accounts only for professional communication.
- Personal devices may not be used to contact students.
- Staff must not take photographs, videos or recordings of pupils on personal devices. School-related media must only be created using school-approved equipment and stored on approved school systems.
- Internet access is subject to appropriate filtering and monitoring arrangements designed to reduce pupils' exposure to harmful and inappropriate online content.
- Filtering and monitoring arrangements are proportionate to the age, needs and vulnerabilities of pupils and are supported technically by the IT Support Provider / Nominated IT Lead.
- Safeguarding oversight of filtering and monitoring arrangements remains with the DSL.
- No student may use a device to access the internet without staff supervision.

For further detail on restrictions around mobile phones, smart watches, and trackers, staff and students must refer to the TAO Mobile Phone & Smart Device Policy

## Images, Videos, and Recordings

Parental consent is obtained before any student is photographed or recorded. Images are stored securely on the TAO network and never shared externally without prior approval. Consent may be withdrawn at any time.

Any concern involving inappropriate, sexualised, manipulated or AI-generated imagery must be treated as a safeguarding concern and reported to the DSL or DDSL.

## Data Protection and Confidentiality

TAO adheres to all GDPR regulations and ensures that personal data is processed fairly, stored securely, and destroyed appropriately. Staff are trained in secure handling

of personal information, particularly regarding digital data and communication, Staff must follow the TAO Data Protection & Privacy Policy when handling digital information, personal data, images, recordings and electronic communications.

## Monitoring, Evaluation and Review

Online safety arrangements are monitored through safeguarding oversight by the DSL, supported by the IT Support Provider / Nominated IT Lead for technical systems. Key issues, risks and actions are recorded and reviewed as part of whole-school safeguarding assurance.

The effectiveness of the school's filtering and monitoring arrangements is reviewed at least annually. The review records checks undertaken, issues identified and any action required.

## Emerging Risks

TAO recognises the increasing risks associated with emerging technologies, including smart trackers, smart watches, generative AI, AI chatbots, deepfakes, image-generation tools, nudification tools, virtual and augmented reality, and peer-to-peer transfer systems such as Bluetooth or AirDrop. Staff remain alert to the use of technology for grooming, exploitation, coercion, harassment, image-based abuse, cyberbullying, radicalisation and other forms of online harm. Any identified misuse which raises a safeguarding concern will be managed in accordance with the Safeguarding & Child Protection Policy

Staff remain alert to radicalisation through online and algorithm-driven content, including AI-generated extremist material, right-wing extremism and misogyny-driven radicalisation.

## Legal & Statutory Framework

This policy has been developed with reference to the following legislation and guidance:

- Children Act 2004
- Data Protection Act 2018 & UK GDPR
- DfE Teaching Online Safety in Schools (2019)
- Education (Independent School Standards) Regulations 2014 (as amended) – Part 3
- Keeping Children Safe in Education (KCSIE) 2026
- Online Safety Act 2023
- Counter-Terrorism and Security Act 2015 and current Prevent Duty guidance
- Working Together to Safeguard Children 2026

## Version Updates

| Version | Date | Author | Review / Changes | Approved By |
|---|---|---|---|---|
| 1.2 | 07/09/2026 | Daniel Giblin | Published | Headteacher / Proprietor |

Updated for KCSIE 2026; strengthened filtering and monitoring arrangements; clarified DSL and IT responsibilities; expanded emerging technology and AI risks; aligned incident reporting and policy cross-references / Proprietor