# Online Safety Policy

**Version control**

| **Scope: Applicable to all Trust Schools** | |
|---|---|
| Date approved by the Board: | Autumn 2026 |
| Review date: | Autumn 2027 |
| Union Status: | *N/A* |
| Statutory or non-statutory: | Non-statutory policy supporting statutory safeguarding duties |
| Author/Reviewer and date: | … |

# 1. Purpose and scope

Online safety is an integral part of safeguarding. Children may experience harm online or face-to-face, and online activity may facilitate or intensify harm occurring offline.

This policy explains how Equals Trust and its schools address the four categories of online risk identified in Keeping Children Safe in Education 2026:

- **content**
- **contact**
- **conduct**
- **commerce**

It applies to all pupils and adults working or volunteering in or on behalf of the Trust. It covers school systems and devices, school-related use of personal devices, and online behaviour outside school where this raises a safeguarding concern or affects the school community.

This policy does not repeat the Trust's wider requirements for safeguarding, staff conduct, artificial intelligence, data protection, filtering and monitoring, technical security or acceptable use. These are contained in the related policies and documents listed in section 7.

# 2. The four categories of online risk

## 2.1 Content

Content risk is exposure to illegal, inappropriate, misleading or harmful material.

Examples include:

- sexual, violent or distressing material, including content promoting self-harm, suicide or eating disorders;
- discriminatory, misogynistic, hateful, extremist or radicalising material;
- misinformation, disinformation, harmful online challenges or material linked to criminal activity; and
- inaccurate, manipulated or AI-generated content.

The school will help pupils recognise, question and report harmful or unreliable content.

## 2.2 Contact

Contact risk arises through interaction with other people or with technology designed to simulate human interaction.

Examples include:

- grooming, exploitation, coercion, manipulation or intimidation;

- pressure to share personal information, images or money;
- adults posing as children, harmful peer contact or radicalising contact; and
- financial exploitation, extortion or manipulative interaction with chatbots or automated services.

The school will help pupils protect personal information, recognise unsafe contact, block or end unwanted communication and seek help from a trusted adult.

Pupils will be encouraged to report concerns even if they have broken a rule, used an age-restricted service or initially participated willingly.

## 2.3 Conduct

Conduct risk concerns behaviour online and its effect on the individual or others.

Examples include:

- online bullying, harassment, abuse, discriminatory or threatening behaviour;
- harmful sexual behaviour or sharing nude or semi-nude images;
- taking, altering or sharing images without consent, including AI-generated or manipulated images;
- impersonation, fake accounts or sharing private or harmful information; and
- attempts to bypass school security controls.

The same standards of behaviour apply online and offline. Online incidents involving pupils will be managed through the school's safeguarding, behaviour and anti-bullying arrangements.

A child who has harmed another child may also have unmet safeguarding needs and will be supported appropriately.

## 2.4 Commerce

Commerce risk concerns financial and commercial activity online.

Examples include:

- phishing, financial scams, identity theft or financial exploitation;
- gambling, gambling-like activity, subscription traps or pressure to make in-app purchases;
- inappropriate advertising and persuasive online design; and
- fraudulent investment or cryptocurrency schemes, extortion, or offers involving illegal goods or services.

## 3. Education and prevention

The school will provide age-appropriate and inclusive online safety education through the curriculum and wider safeguarding activity.

Pupils will be taught to:

- recognise risks involving content, contact, conduct and commerce;
- use technology safely and respectfully and protect personal information;
- question unreliable or manipulated content;
- understand consent, privacy and appropriate image sharing;
- recognise bullying, grooming, coercion and exploitation; and
- block and report harmful content or contact and know how to seek help.

Teaching will reflect pupils' ages, understanding, needs and vulnerabilities, including the needs of pupils with SEND.

The school will provide parents and carers with appropriate information and signposting to help reinforce online safety at home.

## 4. Filtering and monitoring

The Trust and its schools will maintain appropriate filtering and monitoring arrangements in accordance with the Child Protection Policy and relevant technical standards and procedures.

Filtering and monitoring support, but do not replace, effective supervision, education, professional curiosity and safeguarding judgement.

Concerns about harmful content, monitoring alerts, attempts to bypass controls or weaknesses in the school's systems must be reported through the relevant safeguarding or technical reporting route.

Detailed responsibilities, technical requirements and review arrangements are contained in the Trust's filtering and monitoring arrangements and are not repeated in this policy.

## 5. Reporting concerns

Any concern about a child's online safety must be treated as a safeguarding concern and reported promptly to the Designated Safeguarding Lead or a deputy.

Concerns will be recorded and managed under the school's established safeguarding procedures. A separate online safety recording system is not required where the safeguarding record captures the concern, decisions, actions and outcome.

Staff must not investigate suspected abuse or illegal online activity themselves. They must preserve available evidence without searching for, copying or forwarding illegal material.

Concerns involving an employee, volunteer, contractor or other adult working with children must be reported under the Trust's procedures for managing allegations and low-level concerns.

Where an incident does not meet a safeguarding threshold, it may be addressed under the Behaviour Policy, Anti-Bullying Policy, Staff Code of Conduct or another relevant procedure.

## 6. Responsibilities

The **Trust Board and local governing bodies** will seek assurance that online safety is addressed effectively through the Trust's safeguarding, curriculum, and filtering and monitoring arrangements, in accordance with the Trust's Scheme of Delegation.

The **Headteacher** is responsible for ensuring that this policy is implemented within the school.

The **Designated Safeguarding Lead** has lead responsibility for safeguarding and child protection, including online safety.

**Staff and volunteers** must remain alert to online harm, supervise pupils' use of technology appropriately and report concerns promptly.

**Pupils** are expected, according to their age and understanding, to use technology safely and respectfully, follow school requirements and tell a trusted adult if something online worries them.

Professional boundaries, staff communication, personal devices, use of AI and consequences for staff misconduct are governed by the Staff Code of Conduct and the Artificial Intelligence (AI) in Education Policy and are not repeated here.

## 7. Related policies and documents

This policy should be read alongside the current versions of the:

- Child Protection Policy;
- Staff Code of Conduct;
- Behaviour Policy;
- Anti-Bullying Policy;
- Artificial Intelligence (AI) in Education Policy;
- Data Protection Policy;
- Trust filtering and monitoring arrangements and relevant technical and cyber-security procedures;
- Acceptable Use Agreements;
- School mobile-phone arrangements;
- RSHE/RSE and relevant curriculum policies; and
- Managing Allegations and Low-Level Concerns procedures.