



INSPIRE
Connected Communities Trust



Online Safety Policy



1. Scope

This policy outlines Inspire Connected Communities Trust's commitment to safeguarding all pupils, children, staff, governors, volunteers and visitors in relation to online safety. It ensures:

- A consistent Trust-wide approach to online safety.
- Protection from online harm including grooming, exploitation, extremism, manipulation, discrimination, bullying, and sexual harassment.
- Compliance with statutory duties and DfE expectations.
- Clear procedures for prevention, identification and response to concerns.
- A progressive curriculum that builds digital resilience.
- Robust filtering, monitoring and governance arrangements.

This policy applies to all Trust settings including specialist schools and Children's Care Home, recognising the additional vulnerabilities of SEND pupils.

2. Ethos

We commit to:

- Providing safe, respectful and inclusive environments where pupils can develop socially, emotionally and academically.
- Ensuring every child feels heard, understood and protected.
- Promoting safe use of digital technologies, mobile devices and emerging technologies (including Artificial intelligence, AI).
- Building strong partnerships with parents and professionals.
- Embedding a safeguarding culture where all staff recognise online risks as part of wider safeguarding responsibilities.

3. Legal & Statutory Framework

This policy reflects the latest guidance including:

- Keeping Children Safe in Education (KCSIE) 2025
- Working Together to Safeguard Children 2026
- DfE Filtering & Monitoring Standards 2024-26
- DfE (2023) Searching, Screening and Confiscation: Guidance for Schools (updated July 2023)
- UKCIS "Sharing Nudes and Semi-Nudes" 2023
- DfE Generative AI product-safety expectations (2025)
- RSHE Guidance 2020
- Data Protection Act 2018 and UK GDPR



- The Prevent Duty (updated 2024)
- Education Acts 1996, 2006, 2011

Schools must evidence annual review of online safety risks as required in KCSIE 2025.

4. Roles and Responsibilities

4.1 Trust Board:

- Approves the policy and ensures compliance.
- Receives termly safeguarding reports including online safety.
- Ensures filtering & monitoring meets statutory standards.
- Ensures contextual safeguarding for SEND and vulnerable pupils.

4.2 Local School Committees:

- Understand online risk in their settings.
- Review online safety logs.
- Ensure adaptation of online safety for all SEND pathways, EAL and vulnerable pupils.

4.3 Headteachers:

- Ensure consistent implementation.
- Ensure all staff are trained annually.
- Ensure robust systems (filtering/monitoring) are in place.
- Report concerns to the Trust.

4.4 Designated Safeguarding Lead:

- Lead responsibility for online safety.
- Maintain logs and analyse trends.
- Manage incidents including sexual harassment, cyber-bullying and harmful content.
- Liaise with police, CEOP and external agencies.
- Deliver staff training and updates.
- Lead annual online safety risk assessments.

4.5 ICT & Technical Teams:

- Maintain compliant filtering and monitoring systems.
- Prevent access to harmful content including extremist material and illegal images.
- Monitor network activity and notify DSLs of flagged concerns.
- Conduct regular security checks and maintain cyber-security protocols.



4.6 All Staff:

- Follow Acceptable use policy (AUP) and safeguarding procedures.
- Report concerns immediately.
- Model safe digital behaviour.
- Respond appropriately to online sexual harassment or harmful communications.

4.7 Parents/Carers:

- Support safe online use at home.
- Engage with school communications and training.
- Report concerns promptly.

4.8 Visitors:

- Must comply with Trust AUPs when accessing systems.

5. Online Safety Education for Pupils

Education is delivered through Computing, PSHE/RSHE, Life Skills and tailored SEND provision.

Pupils and Children are taught to:

- Think critically about digital content.
- Understand risks related to fake news, deepfakes and manipulated content.
- Recognise grooming, exploitation, online radicalisation and coercion.
- Understand healthy online relationships.
- Manage privacy settings and protect personal information.
- Identify scams, commercial exploitation and fraud.
- Report concerns safely using trusted adults, DSLs or CEOP.
- Understand misinformation disinformation and conspiracy theories

The Trust adopts the Four Cs model:

- Content – exposure to harmful material.
- Contact – interactions with others including grooming.
- Conduct – harmful behaviours such as cyberbullying.
- Commerce – online scams, microtransactions, targeted advertising.

AI Safety:



- Pupils learn appropriate use of generative AI.
- They are taught about deepfake risks and AI manipulation.
- Schools must risk assess new AI tools prior to use.
- Pupils must never input personal data into AI tools.

6. Parent/Carer Education

The Trust will:

- Provide workshops, newsletters and website resources.
- Communicate curriculum content and filtering/monitoring systems.
- Support parents to set controls on home devices.
- Inform parents when pupils engage in online learning platforms.
- Share signposting for CEOP, Internet Watch Foundation and NSPCC guidance.

7. Cyber-Bullying

Cyber-bullying includes harassment, intimidation, threats, manipulation, non-consensual sharing of images, catfishing, group exclusion and AI-generated bullying (e.g., deepfakes). AI-generated intimate images (e.g., deepfakes), are now recognised within sexual-image safeguarding terminology.

The Trust will:

- Educate pupils on recognising and reporting cyber-bullying.
- Support victims with tailored interventions.
- Respond according to Behaviour and Safeguarding Policies.
- Involve police where material is illegal or harmful.
- Contain incidents through swift action.
- Maintain clear records of incidents and actions taken.

8. Searching, Screening & Confiscation

This section aligns with KCSIE 2025 guidance on searching, screening and confiscation.

Schools will follow DfE 2023 guidance. Staff authorised by the Headteacher may search a device if:

- There is reasonable suspicion it contains harmful, illegal or prohibited material.
- It poses a risk to pupils or staff.

If indecent images of a child are suspected:



- Staff must NOT view the image.
- The DSL must be notified immediately.
- Police involvement will be sought where appropriate.

Devices may be handed to police where material is illegal or related to an offence.

9. Acceptable Use of ICT Systems

All users must sign AUPs appropriate to their role. Expectations include:

- Only educational or work-related use.
- No access to inappropriate content.
- Use of School/Care Home/Trust systems only for professional purposes.
- Agreement to monitoring of activity.

Schools must maintain up-to-date AUPs for pupils (primary & secondary), staff, volunteers and visitors.

10. Staff Use of Work Devices Off-Site

Staff must:

- Keep devices encrypted and password protected.
- Ensure screens lock automatically.
- Avoid storing sensitive data on personal devices.
- Install updates and security patches promptly.
- Report any loss, compromise or breach immediately.
- Never allow family members to use School/Trust-owned devices.

11. Responding to Misuse

The Trust responds proportionately to misuse:

For pupils / children:

- Behaviour and safeguarding policies determine actions.
- Support and education are prioritised.

For staff:

- Misuse may trigger disciplinary procedures.
- Potential safeguarding or data breach actions may apply.



All incidents must be recorded and monitored for patterns.

12. Training

Training requirements:

- All staff receive safeguarding and online safety training annually.
- New staff receive induction training covering online safety.
- DSLs receive formal training at least every 2 years plus annual updates.
- Governors receive safeguarding training including online safety.
- Volunteers receive appropriate level updates.

Training covers:

- Online grooming, exploitation and radicalisation.
- AI risks including deepfakes.
- Recognising online sexual harassment.
- Filtering and monitoring expectations.
- Responding to disclosures and safeguarding escalation routes.
- Misinformation, disinformation and conspiracy theories.
- AI-related risks (deepfakes, manipulation, generative AI).

13. Monitoring, Assurance & Review

Trust monitoring includes:

- Annual online safety risk assessment per school.
- DSL monitoring of logs and incident analysis.
- ICT-led audit of filtering and monitoring systems.
- Annual review of filtering and monitoring systems in line with updated DfE standards, including assessment of real-time scanning and illegal-content filter enforcement.
- Governance review through termly reporting.

This policy is reviewed annually by Trust safeguarding leadership and approved by the Trust Board.
Last reviewed March 2026.