



IRLAM PRIMARY SCHOOL ONLINE SAFETY POLICY 2026-2027

Updated: October 2026

Review Date: September 2027

Introduction

Irlam Primary School is committed to safeguarding and promoting the welfare of children. Online safety is an integral part of this responsibility.

This policy is informed by Keeping Children Safe in Education 2026, Department for Education filtering and monitoring standards and current data protection requirements. It should be read alongside the school's child protection, behaviour, anti-bullying, acceptable use, staff code of conduct, data protection and remote education policies, and relevant Trust procedures.

Scope of Policy

This policy applies to pupils, staff, governors, volunteers, parents, visitors and community users. It covers school devices, networks, personal devices on site and online behaviour that impacts school life.

Our Approach to Online Safety

The school uses a three-layer safeguarding approach:

- Filtering – blocking harmful or inappropriate content
- Monitoring – identifying concerns through supervision, activity reports and technical alerts
- Education – teaching pupils safe and responsible online behaviour

The four areas of online risk

The school considers four areas of online risk when planning education, filtering and monitoring, staff training and responses to concerns:

Content – exposure to illegal, inappropriate or harmful material, including pornography, violence, self-harm, suicide, racist, hateful or misogynistic material, extremist content and misinformation.

Contact – harmful interactions with others online or with AI applications that simulate human interaction, including grooming, exploitation, impersonation and pressure from peers or adults to share personal information or images.

Conduct – online behaviour that may cause harm, including cyberbullying, harassment, sharing harmful or private material, and creating or sharing inappropriate images, including images generated using AI.

Commerce – financial and commercial risks, including scams, phishing, online gambling, misleading advertising and pressure to make in-game or app purchases.

Teaching about these risks will be age appropriate and adapted to pupils' needs. Pupils will be taught to recognise concerns, protect personal information and seek help from a trusted adult. Staff will report concerns promptly through the school's safeguarding procedures.

Filtering and Monitoring Systems

The school uses Senso.cloud as part of its monitoring arrangements. Monitoring complements filtering and staff supervision; it does not itself block harmful material or guarantee that every risk will be detected. IT support must maintain an accurate record of the filtering and monitoring products, coverage and limitations.

The DSL and DDSL receive monitoring alerts during the school day and review and action them immediately as they come through. The DSL and DDSL will agree arrangements for absence cover and any out-of-hours alerts. Users and families will be informed about monitoring and its limitations.

Filtering will block illegal and harmful material without unnecessarily restricting learning. Staff must report inappropriate access, excessive blocking and failures; authorised changes must be recorded. Personal mobile data may bypass school controls.

The responsible senior leader, DSL and IT support will review provision annually with governor oversight, and after significant changes or incidents. Checks must cover relevant devices, accounts and locations, including school-managed devices used off site. Records will show dates, testers, results and actions.

Roles and Responsibilities

Governing Body

- Oversee this policy within Trust governance arrangements
- Assign a governor to oversee filtering and monitoring
- Receive assurance about reviews, training, incidents and resulting actions

Headteacher

- Ensure this policy is implemented and resources are available
- Ensure a senior leader is assigned responsibility for filtering and monitoring
- Ensure staff training, technical support and incident response arrangements are effective

Designated Safeguarding Lead and Online Safety Lead

Lindsey Caplan leads the safeguarding response to online concerns, coordinates training and keeps safeguarding records. The DSL works with senior leaders and IT support on risk assessment and system reviews. A deputy DSL provides cover when needed; technical maintenance remains an IT responsibility.

IT support

IT support maintains controls, supplies reports, completes checks and remedies faults. It must promptly refer safeguarding concerns to the DSL and support documented reviews. Technical service details and assigned contacts will be recorded internally.

Staff

- Follow acceptable use and staff conduct requirements
- Supervise device use and check resources before lessons
- Teach online safety and know how to report concerns
- Report safeguarding concerns promptly to the DSL or deputy and technical faults to IT support

Pupils

- Follow pupil Acceptable Use rules
- Report anything worrying or unsafe

Parents/Carers

- Support safe use at home
- Engage with school guidance and communication

Staff training

Induction and regular safeguarding training will include online risks, filtering and monitoring responsibilities, alert responses and reporting. Updates will be provided at least annually and sooner when risks change. Governors and staff with specialist responsibilities will receive relevant training.

Online Safety Education

Online safety is embedded through the computing curriculum, PSHE, assemblies, Safer Internet Day and regular staff and parent communication.

Teaching covers the four Cs through computing, PSHE and relationships education, using age appropriate examples of privacy, kindness, boundaries, cyberbullying, misleading information, scams, advertising and help seeking. Staff will explain age restrictions and how to question online claims. Resources will be checked for suitability; one-off events will supplement regular teaching.

Support will be adapted for pupils with SEND, communication needs or other vulnerabilities. Pupils will practise telling a trusted adult, including if a first disclosure is not heard. Reporting must be accessible and children will be reassured that abuse is never their fault.

Working with parents and carers

The school will share practical advice on controls, privacy, age restrictions and reporting. Families will be told which platforms children are expected to use and how school contact will take place. Parents should report school-related concerns through normal school channels; urgent danger must not wait for a school reply.

Acceptable Use Expectations

Users must:

- Use school systems appropriately
- Communicate respectfully
- Protect passwords
- Report concerns

Users must not:

- Access illegal or harmful material
- Bypass filtering
- Use personal social media to contact pupils
- Share confidential information

Mobile Phones and Personal Devices

Pupils must not access personal phones or connected devices during the school day, including breaks and lunchtime. Any device brought to school must be switched off and stored securely under school arrangements. The Headteacher may authorise specific exceptions for medical needs, disability adjustments or other justified circumstances, with agreed safeguards. Trip arrangements will be communicated in advance.

Staff must not use personal devices for personal purposes while supervising children. Emergency or specifically authorised work use must follow school procedures and maintain effective supervision. Visitors must follow staff instructions and must not photograph or record pupils without authorisation.

Images, Photos and Videos

Staff must use school-authorised equipment and accounts to capture, store or share pupil images. Personal storage and unauthorised sharing are prohibited. The school will establish a lawful basis for each use, explain it in privacy information and check recorded parental permissions, objections and any safeguarding restrictions before publication. Where consent is the lawful basis, it must be valid and withdrawal respected. Children's wishes will also be considered. Images must not reveal unnecessary identifying information.

Parents and visitors must follow the school's photography arrangements. Images containing other pupils must not be published or shared online without appropriate permission. Images will be retained and deleted under school or Trust retention procedures.

Social Media

Staff must maintain professional boundaries and must not add pupils or parents to personal accounts. School platforms must be used for official communication only.

Remote education

Remote teaching and pastoral contact must use approved school platforms and accounts. Staff will explain safe participation, privacy and reporting to families. Live sessions must follow school safeguarding arrangements; any one-to-one session requires senior leader approval and an assessment of safeguards. Concerns arising remotely follow the same reporting procedures as those in school.

Artificial intelligence

The use of artificial intelligence in school is covered by the school's separate AI policy. All staff must follow that policy and report any safeguarding concerns arising from AI use to the DSL or DDSL.

Incident Reporting Procedure

1. Make the child safe and report promptly to the DSL or deputy. Call 999 if there is immediate danger. Any staff member may make a necessary safeguarding referral; do not delay because a lead is unavailable.
2. Listen calmly, do not promise secrecy or investigate through leading questions, and record the concern and the child's words on CPOMS.
3. The DSL assesses risk, coordinates support and decides on referrals to children's social care, police or other services. Parents will normally be informed unless this could increase risk or compromise safeguarding action.
4. IT support addresses technical issues without replacing the safeguarding response. Actions, decisions and outcomes must be recorded and followed up.

5. Concerns about staff go to the Headteacher; concerns about the Headteacher follow the child protection policy's route to the Chair of Governors or appropriate Trust lead.

Nudes and semi nudes

Report immediately to the DSL, including suspected AI-generated or altered sexual images of children. Staff must not ask pupils to send images, or copy, print, save or forward them. Do not deliberately view imagery or ask a child to show it. Exceptional viewing, device searches and deletion decisions must be led by the DSL under current national guidance and school procedures. Record the report without attaching the imagery. Unavoidable viewing must be reported. The DSL will consider coercion, adult involvement and exploitation, arrange referrals where needed and support affected children.

Sanctions

Behaviour consequences will be proportionate, follow school policy and take account of age, needs and safeguarding circumstances. Support and protection take priority for children experiencing abuse. Staff breaches will follow Trust procedures. The DSL or Headteacher will consider police involvement and other referrals in line with safeguarding guidance; suspected criminal behaviour will not be managed solely through school sanctions.

Data Protection

Personal data must be handled under current data protection law and school or Trust policies. Use approved systems, strong individual passwords and appropriate access controls. Monitoring records must be restricted to authorised staff and retained proportionately. New services must undergo safeguarding and data protection checks, including a data protection impact assessment where required.

Report suspected phishing, account compromise, lost devices or data breaches immediately to school leaders, IT support and the data protection lead. They will contain the incident, assess safeguarding impact and arrange any required notifications. Technical security, updates and backups must be maintained through IT procedures.

Monitoring and Review

This policy and the school's online safety approach will be reviewed at least annually, supported by an assessment of pupils' risks, incidents, pupil and parent feedback, training needs and technical findings. Significant incidents, new technology or guidance changes will prompt an earlier review. Approval will follow school and Trust governance arrangements. The approved policy will be available on the school website.

Guidance informing this policy

Keeping Children Safe in Education 2026; DfE filtering and monitoring standards; DfE teaching online safety; DfE mobile phones in schools; UKCIS sharing nudes and semi nudes; DfE generative AI in education; ICO photographs in schools