



Ludlow Church of England School

Online Safety (E-Safety) Policy

Approved by	Local Governing Body
Date Approved	November 2023
Last Revised	October 2025
Date Revised	May 2026
Next review Date	May 2027

Contents

1. Aims
2. Legislation and guidance
3. Roles and responsibilities
4. Educating pupils about online safety
5. Educating parents/carers about online safety
6. Cyber-bullying (including searching, screening and confiscation)
7. Acceptable use of the internet in school
8. Pupils using mobile devices in school
9. Staff using work devices outside school
10. How the school will respond to issues of misuse
11. Training
12. Filtering & Monitoring arrangements
13. Links with other policies

1. Aims

The school is committed to ensuring that all members of its community are able to use technology safely, responsibly and respectfully. Online safety is treated as a core safeguarding priority and is addressed through curriculum, culture, behaviour expectations, training and effective technical controls.

This policy aims to:

- have robust, proportionate systems in place to protect pupils, staff, volunteers and governors from online harm
- identify, understand and support pupils who may be at greater risk online (including vulnerable pupils and pupils with SEND)
- deliver a whole-school approach to online safety that empowers pupils and adults to make safe choices and to report concerns
- establish clear reporting routes and escalation pathways for online safety concerns and incidents
- maintain a safeguarding culture where pupils feel listened to and supported, and where staff maintain professional curiosity.

The four key categories of online risk recognised by the Department for Education are:

- Content: exposure to illegal, inappropriate or harmful material (including pornography, extremist content, hate content, self-harm/suicide content, and misinformation/disinformation).
- Contact: harmful interaction with others online, including grooming, exploitation, coercion, harassment or peer-on-peer abuse.
- Conduct: behaviour that increases risk or causes harm, including cyber-bullying, harassment, sharing indecent images, or misuse of technology.
- Commerce: risks relating to financial exploitation, scams, phishing, gambling or inappropriate advertising.

2. Legislation and guidance

This policy is informed by the most recent version of Keeping Children Safe in Education (KCSIE) and should be read alongside the School's Safeguarding Policy.

It has regard to Department for Education (DfE) guidance including:

- Teaching online safety in schools
- Filtering and monitoring: meeting digital and technology standards in schools and colleges
- Preventing and tackling bullying and cyber-bullying
- Relationships and sex education (RSE) and health education (secondary)
- Searching, screening and confiscation

- Protecting children from radicalisation and extremism.

It reflects relevant legislation including (but not limited to) the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Education Act 2011 and the Equality Act 2010, and it takes account of the National Curriculum Computing programmes of study.

3. Roles and responsibilities

Online safety is a shared responsibility. Roles are summarised below; more detail is contained in safeguarding and IT procedures.

3.1 Local Governing Body (LGB)

The Local Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The LGB will ensure online safety remains a running theme within safeguarding governance, including oversight of filtering and monitoring effectiveness and staff training.

The Link Governor for Safeguarding oversees online safety.

3.2 Headteacher

The Headteacher is responsible for ensuring this policy is implemented consistently and that staff understand and follow online safety expectations and reporting routes.

3.3 Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety and safeguarding response to online harms. Online safety concerns and incidents are recorded via MyConcern. The DSL works with the ICT team and senior leaders to review risks, respond to incidents and provide regular training and updates to staff.

3.4 ICT Manager / ICT Technician

The ICT Manager/Technician is responsible for day-to-day operation of filtering and monitoring systems, maintaining secure systems and escalating safeguarding-relevant alerts to the DSL.

3.5 Staff and volunteers

All staff and volunteers are responsible for following acceptable use expectations, maintaining professional boundaries online, supervising use of technology appropriately, and reporting concerns promptly via MyConcern and to the DSL.

3.6 Parents/carers

Parents/carers are expected to support the school's approach to online safety and raise concerns promptly with the school.

3.7 Visitors and community users

Visitors who access School ICT systems are expected to comply with acceptable use expectations where applicable.

4. Educating pupils about online safety

Online safety is taught as part of the Computer Science curriculum and wider school curriculum (PSHE, assemblies and pastoral/form time), and is planned to be progressive and age-appropriate across Key Stage 3 and Key Stage 4.

In Key Stage 3 pupils are taught to:

- use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- recognise inappropriate content, contact and conduct and know how to report concerns.

In Key Stage 4 pupils are taught to:

- understand how changes in technology affect safety, including new ways to protect online privacy and identity
- report a range of concerns and seek support.

By the end of secondary school, pupils will understand:

- rights, responsibilities and expectations online, and that behaviour standards apply online as well as offline
- the risks of sharing content and the difficulty of removing material once shared
- how and where to seek help and report concerns (in school and externally where appropriate)
- the harms associated with pornography and sexually explicit material
- the law and safeguarding implications relating to indecent images of children and non-consensual sharing
- how misinformation, disinformation and scams can cause harm, including risks of radicalisation or exploitation
- how to recognise and respond to bullying, harassment, coercive or controlling behaviour online
- how AI and deepfakes can be used maliciously and how to report concerns.

Teaching is adapted where necessary for pupils with SEND and for vulnerable pupils, reflecting the importance of a personalised approach to safeguarding.

5. Educating parents/carers about online safety

The school raises parents/carers' awareness of online safety through the school website, letters/communications home and the half-termly newsletter. This policy is available to parents/carers via the school website.

The school will let parents/carers know:

- what systems the school uses to filter and monitor online activity
- what pupils are being asked to do online, including platforms used and where interaction may occur
- how to raise concerns and how the school will respond.

Concerns about online safety should be raised in the first instance with any member of staff, the Headteacher and/or the DSL.

6. Cyber-bullying (including searching, screening and confiscation)

Cyber-bullying is addressed in line with the Behaviour Policy and Child-on-child Abuse policy. Cyber-bullying includes harassment or intimidation via social media, messaging, gaming platforms or other online services.

The school will:

- teach pupils what cyber-bullying is and how to report concerns
- support pupils who are affected and take proportionate action to address harmful behaviour
- record incidents and outcomes via MyConcern (and behaviour systems where applicable)
- consider safeguarding thresholds and referral to external agencies where necessary.

6.3 Examining electronic devices

The Headteacher and staff authorised by the Headteacher may search and confiscate devices where there are reasonable grounds to suspect a prohibited item or evidence of an offence, or where the item is banned under school rules. Decisions are made proportionately and with safeguarding considerations. Where there is reasonable suspicion of indecent images of a child, staff will not view the image, will secure the device, and will report immediately to the DSL who will determine next steps in line with national guidance.

6.4 Artificial intelligence (AI)

The school recognises that generative AI can support learning but may also increase safeguarding risks (e.g., deepfakes, harassment, misinformation). Misuse of AI to harm or

humiliate others will be addressed through safeguarding and behaviour procedures. Where the School introduces AI tools, risks will be considered and mitigated appropriately.

7. Acceptable use of the internet in school

All pupils, staff, governors, volunteers and visitors are expected to comply with acceptable use expectations when using School ICT systems or internet access (when logging on to the school system). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use must be for educational purposes or to fulfil duties of an individual's role.

The school monitors websites and online activity on its systems and uses filtering to restrict access to harmful, inappropriate or illegal material.

8. Pupils using mobile devices in school

The use of mobile phones and other smart devices (including devices capable of sending or receiving messages, accessing the internet, or recording audio or video) by pupils is not permitted during the school day, including:

- lessons
- movement between lessons
- break times
- lunchtimes

This restriction is in place to safeguard pupils, reduce distraction, prevent online harm (including cyberbullying and misuse of images), and support a calm and focused learning environment, in accordance with Keeping Children Safe in Education and the school's safeguarding duties

Any breach may result in sanctions in line with the Behaviour Policy.

9. Staff using work devices outside school

Staff take appropriate steps to keep school devices secure when used off-site. This includes strong password protection, device locking, installing updates promptly, and using encryption where available (for example, BitLocker on Windows devices).

Work devices must be used solely for work activities and in accordance with acceptable use and the Staff Code of Conduct.

If staff have concerns over device security, they should seek advice from the ICT Manager / Technician).

10. How the school will respond to issues of misuse

Where a pupil misuses the School's ICT systems or internet, the school will follow the procedures set out in the Behaviour Policy and ICT/acceptable use arrangements. Actions taken will be proportionate to the circumstances, nature and seriousness of the incident.

Where a staff member misuses ICT systems or the internet or misuses a personal device in a way that constitutes misconduct, this will be managed in line with the Staff Code of Conduct and disciplinary procedures.

The school will consider whether serious incidents, including those involving illegal activity or content, should be reported to the police and/or other agencies.

11. Training

11.1 Staff, governors and volunteers

All new staff members receive online safety training as part of induction. All staff receive refresher training at least annually as part of safeguarding training and receive updates as required through briefings, emails and staff meetings.

Training includes the understanding that technology is a significant component in safeguarding and wellbeing issues and that children can be abused online and offline. Staff are supported to recognise signs of online abuse, including child-on-child abuse, and to respond and record concerns appropriately.

The DSL and deputies undertake safeguarding training (including online safety) at least every two years and update their knowledge regularly.

Governors receive safeguarding and online safety training appropriate to their role. Volunteers receive appropriate training and updates, where applicable.

11.2 Pupils

All pupils receive age-appropriate education on safe internet use, including cyber security basics (passwords, social engineering, safe reporting), and safeguarding risks such as cyberbullying and online radicalisation.

12. Filtering & Monitoring arrangements

The school uses Smoothwall as its web filtering system. This system supports safeguarding by helping to prevent access to harmful/illegal content (filtering) and by generating alerts/reports about concerning activity (monitoring).

The Designated Safeguarding Lead (DSL) is responsible for recording, monitoring and taking appropriate action in response to all alerts generated through Smoothwall. The DSL logs safeguarding issues related to online safety via MyConcern.

All staff are trained so they are clear on:

- their roles and responsibilities in relation to filtering and monitoring (including classroom supervision of pupil screens)

- how to report safeguarding and technical concerns, including where unsuitable material may have been accessed, where restrictions appear unreasonable, or where there may be attempts to bypass controls
- how to inform the DSL/ICT team if teaching content may create unusual activity on filtering logs (to avoid misinterpretation while safeguarding remains paramount).

Filtering and monitoring arrangements are reviewed at least annually for effectiveness, with interim checks and reviews as needed. Decisions about safeguarding responses to monitoring alerts are led by the DSL in collaboration with the ICT team.

13. Links with other policies

This policy should be read alongside:

- Safeguarding Policy
- Behaviour for learning policy
- Staff Code of Conduct
- Data Protection policy and privacy notices
- Complaints procedure.

This policy will be reviewed annually by the DSL. The review will be supported by an annual risk assessment that considers and reflects the evolving risks and harms related to technology.