Nottinghamshire County Council The Key > Leaders

Mapperley Plains Primary School

Online Safety Policy

Non-Statutory

Approved by	Academic Committee
Approval date	Autumn 2026
Review date	Autumn 2027
Version	V1

Inspiring learners. Shaping futures.

1. Aims

Mapperley Plains Primary and Nursery School aims to provide a safe, purposeful and age-appropriate digital environment. Online safety is treated as an integral part of safeguarding, behaviour, curriculum, staff conduct, data protection and the school's wider culture.

- have robust processes to protect children, staff, volunteers and governors online
- identify and support children who may be at greater risk of online harm, including children with SEND and other vulnerabilities
- teach children to use technology safely, respectfully, responsibly and critically
- make clear how concerns, incidents and technical failures are reported, recorded, escalated and reviewed
- ensure filtering and monitoring arrangements are effective and reviewed at least annually
- set clear expectations for the safe use of artificial intelligence (AI), mobile technology and online services.

The four key categories of online risk

Our approach is based on the four categories of risk set out in national safeguarding guidance:

- **Content:** exposure to illegal, inappropriate or harmful material, including pornography, extreme sexual or physical violence, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation and conspiracy theories.
- **Contact:** harmful interaction with other users, or generative AI applications that simulate interaction, including peer pressure, commercial approaches and adults posing as children or young adults to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** online behaviour that increases the likelihood of harm, including online bullying, abusive messages and making, sending or receiving explicit images, including images generated or altered using AI.
- **Commerce:** risks including online gambling, inappropriate advertising, phishing, scams and other attempts to obtain money or personal information.

2. Legislation and guidance

This policy is based on current Department for Education safeguarding and education guidance, including Keeping Children Safe in Education 2026. It also has regard to guidance and standards on teaching online safety, filtering and monitoring, searching and confiscation, mobile phones in schools, relationships education and health education and protecting children from radicalisation.

It reflects relevant legislation, including the Education Act 1996 (as amended), Education and Inspections Act 2006, Education Act 2011, Equality Act 2010 and Children's Wellbeing and Schools Act 2026. As a maintained primary school, Mapperley Plains also takes account of the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. It will ensure that online safety remains a running and interrelated theme within the school's whole-school approach to safeguarding, curriculum, staff training, the role of the DSL and engagement with parents and carers.

- ensure staff receive online safety training as part of safeguarding training and understand their responsibilities for filtering and monitoring
- ensure staff receive regular online safety updates, at least annually and more often where risks or guidance change
- ensure the school teaches children how to keep themselves and others safe online
- ensure appropriate filtering and monitoring systems are in place on school devices and networks
- receive assurance that senior leaders review the effectiveness of filtering and monitoring at least once every academic year
- consider the DfE filtering and monitoring standards and challenge leaders on whether the school's arrangements meet safeguarding need without unreasonably restricting teaching and learning.

The Safeguarding Link Governor oversees online safety on behalf of the governing body. At the date of this policy, this role is held by Becky Dixon.

All governors are expected to understand this policy and follow the school's acceptable use requirements.

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy and that it is implemented consistently. The Headteacher will also ensure robust cover arrangements are in place when the DSL is unavailable so that safeguarding concerns, including online concerns, are received, monitored and acted on without delay.

3.3 The Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety. Details of the DSL and deputies are set out in the Child Protection Policy. The DSL will:

- lead on understanding the filtering and monitoring systems and processes in place on school devices and networks
- provide governors with assurance that filtering and monitoring arrangements are working effectively and are reviewed regularly
- work with the Headteacher, external ICT support provider and relevant staff to address online safety issues or incidents
- respond to safeguarding concerns identified through filtering and monitoring
- ensure safeguarding and behaviour incidents relating to online safety are recorded appropriately on CPOMS
- ensure cyber-bullying and child-on-child online abuse are dealt with under the appropriate safeguarding, behaviour and anti-bullying procedures
- provide or coordinate online safety training and updates for staff
- liaise with external agencies and services where necessary
- report regularly to the Headteacher and governing body on online safety themes and assurance
- ensure an annual risk assessment considers the online risks faced by children at Mapperley Plains.

3.4 Technical management and external ICT support

The school uses an external ICT support provider to manage and support key aspects of its digital infrastructure. School leaders retain accountability for safeguarding decisions and for ensuring that technical arrangements meet the school's needs.

- appropriate security, filtering and monitoring protections are applied to school devices and networks
- systems are maintained, patched and protected against malware and unauthorised access
- harmful and inappropriate content is blocked without unreasonably restricting legitimate teaching and learning
- technical failures or safeguarding concerns are escalated promptly to the DSL and Headteacher
- changes to filtering, monitoring or access controls are authorised and recorded appropriately.

Staff must not attempt to bypass filtering or monitoring controls. Where legitimate educational access is required, staff must seek approval through the Headteacher or DSL so that the request can be considered and, where appropriate, implemented safely by the school's ICT support provider.

3.5 All staff, agency staff, contractors and volunteers

All adults working in or for the school are responsible for:

- understanding and implementing this policy and the school's acceptable use requirements
- knowing that the DSL leads on filtering and monitoring and reporting any failure, gap or concern immediately
- following school procedures when using online services, cloud systems and AI tools
- reporting online safety concerns and incidents promptly and accurately
- responding appropriately to reports of sexual violence, sexual harassment and other child-on-child abuse online and offline, maintaining an attitude that "it could happen here"
- protecting personal, safeguarding, SEND, medical and other confidential information when using digital systems.

3.6 Parents and carers

Parents and carers are expected to support the school's online safety expectations, raise concerns promptly and help their child understand the acceptable use arrangements that apply in school. The school will provide signposting to trusted online safety advice and will communicate significant changes in expectations.

3.7 Visitors and members of the community

Visitors and community users who access school ICT systems or internet services must follow this policy and the relevant acceptable use requirements. Access may be restricted or withdrawn where necessary to protect safeguarding, security or school operations.

4. Educating children about online safety

4.1 Curriculum

Online safety is taught through computing, relationships and health education and other curriculum areas where relevant. Teaching is age-appropriate and is adapted where necessary for vulnerable children, victims of abuse and children with SEND.

In Key Stage 1, children are taught to:

- use technology safely and respectfully and keep personal information private
- identify where to go for help and support when they are concerned about online content or contact.

In Key Stage 2, children are taught to:

- use technology safely, respectfully and responsibly
- recognise acceptable and unacceptable behaviour
- identify a range of ways to report concerns about content and contact
- be discerning and critical when evaluating digital content.

By the end of primary school, children will be taught, in age-appropriate ways, about:

- respectful online interaction and how the same principles of respect apply online and face to face, including strategies for resisting pressure to share information or images
- how to evaluate online relationships and information, including the risk that people may pretend to be someone else or pretend to be a child
- the existence and purpose of minimum-age requirements for social media and other online services
- the importance of privacy and location settings and of being cautious about sharing personal information
- the fact that online material can be copied and circulated and may be impossible to remove completely once shared
- how to recognise harmful or upsetting content or contact and where to obtain advice and support
- how AI-generated material, edited images, fake accounts and misleading content can make online information appear convincing when it is not reliable or authentic.

4.2 Practical cyber security skills

Children will receive age-appropriate teaching on safe internet use and basic cyber security, including:

- how people may be tricked into disclosing personal information
- password security and the importance of keeping login details private
- social engineering and phishing
- the physical security of devices and the risks of removable storage
- multi-factor authentication where relevant
- how to report a cyber incident, attack or personal data breach to an adult.

5. Educating parents and carers about online safety

The school will raise awareness of online safety through the school website, newsletters and other communications and will share this policy with parents and carers. Where relevant, online safety may also be discussed through meetings or events with families.

Parents and carers will be informed about:

- the school's approach to filtering and monitoring
- the online services and sites children may be asked to use for learning
- the school's expectations for mobile phones, smartwatches and other personal devices
- the school's expectations for age-appropriate and approved use of AI by children.

Questions or concerns should normally be raised with a member of staff, the Headteacher or the DSL, depending on the nature of the issue.

6. Cyber-bullying and online abuse

6.1 Definition and scope

Cyber-bullying is bullying carried out through digital technology, including social media, messaging, gaming and other online platforms. As with other bullying, it is normally repetitive and intentional and involves an imbalance of power. A harmful online

incident does not need to meet the school's definition of bullying before action is taken: one-off abuse, harassment, sexualised behaviour, threats or safeguarding concerns will still be addressed under the appropriate policy and safeguarding procedures.

6.2 Preventing and responding to cyber-bullying

- children are taught what cyber-bullying and online abuse can look like and how to report it
- staff reinforce respectful online behaviour through the curriculum and wider school culture
- staff, governors and relevant volunteers receive safeguarding training that includes online harm
- parents and carers are signposted to advice on recognising and responding to online harm
- specific incidents are managed through the Behaviour Policy, Anti-Bullying Policy and Child Protection Policy as appropriate
- where illegal, harmful or inappropriate material is involved, the school will take proportionate steps to contain the incident and seek advice or involve external agencies where necessary.

6.3 Searching electronic devices and suspected sexual imagery

The Headteacher and staff authorised by the Headteacher may search for and confiscate electronic devices in accordance with current DfE guidance, the school's Behaviour Policy and safeguarding procedures. Any decision to examine or erase data must be lawful, proportionate and based on a clear reason.

If a member of staff has already seen an image accidentally, they must report this to the DSL and seek support. Complaints about searching or confiscation will be managed through the school's Complaints Policy and Procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are widely available and may be encountered by children, staff and families. They can support learning and productivity but also create safeguarding, accuracy, privacy and conduct risks.

- AI may be used to create convincing fake text, images, audio or video, including deepfakes and sexualised "deep nude" imagery
- AI chatbots can simulate relationships or intimacy and may provide inaccurate, unsafe or harmful advice
- AI-generated or altered content can be used to bully, harass, impersonate or humiliate others
- staff must not input personal data, safeguarding information, SEND or medical information, confidential school information or other sensitive data into public or unapproved AI tools
- children may only use AI tools in school where a member of staff has approved the activity, the tool is appropriate for their age and the use is consistent with data protection and safeguarding requirements
- new or materially different uses of AI by the school will be considered for risk, privacy and safeguarding implications before use.

Misuse of AI will be addressed under the relevant safeguarding, behaviour, anti-bullying, staff conduct, data protection or disciplinary arrangements.

7. Acceptable use of the internet and AI in school

Children, staff, governors, volunteers and other authorised users must follow the definitive acceptable use agreements in the ICT and Acceptable Use Policy. This Online Safety Policy sets the safeguarding expectations that underpin those agreements, including expectations relating to AI, online harm, filtering and monitoring.

Where the two policies overlap, the ICT and Acceptable Use Policy governs operational use of school systems and signed acceptable-use expectations, while this policy governs safeguarding, curriculum and incident response.

8. Mobile phones and smartwatches

Mapperley Plains is a mobile phone-free school. Children are not permitted access to or use of personal mobile phones or communication-enabled smart technology, including smartwatches, during the school day. Any exception must be individually authorised by the Headteacher, for example for an agreed medical or safeguarding need.

Children who have permission to bring a device to school must follow the hand-in, storage and collection arrangements set out in the Mobile Phone and Smartwatch Policy. Devices must not be accessed during lessons, transitions, breaktimes, lunchtimes or wraparound provision unless an agreed exception applies.

9. Staff using work devices outside school

Staff must take reasonable steps to keep school devices and information secure when working away from the school site. This includes:

- using strong passwords and multi-factor authentication where provided
- locking devices when unattended and preventing access by family members or other unauthorised people
- keeping devices physically secure and reporting loss or theft immediately
- using school-approved systems for storing and sharing school information
- not disabling security, filtering, monitoring, encryption or update controls
- not installing unauthorised software or connecting unauthorised hardware
- promptly reporting security concerns, suspected compromise or data breaches.

Staff must follow the ICT and Acceptable Use Policy, Staff Code of Conduct, data protection requirements and the AI controls in this policy when using work devices.

10. How the school will respond to issues of misuse

Responses will be proportionate to the circumstances, nature, seriousness and safeguarding implications of the incident.

- Where a child misuses school ICT systems, the school will use the Behaviour Policy and, where relevant, safeguarding or anti-bullying procedures.
- Where a member of staff misuses school ICT systems, a personal device or an online service in a way that may constitute misconduct, the matter will be considered under the Staff Code of Conduct and appropriate employment procedures.
- Where an incident involves suspected illegal activity, illegal content, significant safeguarding risk or serious harm, the school will seek advice and consider referral to the police, children's social care, the local authority or other relevant agencies.
- Technical failures affecting filtering or monitoring will be treated as safeguarding issues and escalated promptly.

11. Training for staff, governors and volunteers

All new staff receive online safety training as part of induction. All staff receive refresher training at least once each academic year as part of safeguarding training, with additional updates when risks, technology or guidance change.

Training will include, as appropriate:

- the role of technology in safeguarding and wellbeing concerns
- online child-on-child abuse, including abusive or misogynistic messages and non-consensual sharing of nude or semi-nude images, including AI-generated or altered images
- the school's filtering and monitoring arrangements and staff responsibilities
- online radicalisation, misinformation, disinformation, scams and harmful content
- safe and lawful use of AI, including confidentiality and data protection
- how to report and respond to online safety concerns.

The DSL and deputies undertake safeguarding training, including online safety, at least every two years and update their knowledge and skills regularly and at least annually. Governors receive appropriate safeguarding and online safety training. Volunteers receive training and updates proportionate to their role.

12. Monitoring arrangements

The DSL oversees the logging and review of safeguarding and behaviour issues related to online safety. Child-specific safeguarding concerns are recorded on CPOMS. Technical incidents and filtering or monitoring failures are recorded and escalated through the appropriate school and ICT support routes.

This policy will be reviewed annually by the Headteacher and DSL and shared with the governing body. The annual review will be informed by:

- an annual online safety risk assessment
- the annual review of filtering and monitoring arrangements
- patterns and themes from CPOMS, behaviour and technical incident records
- changes to statutory guidance, technology and emerging online risks
- feedback from staff, children, governors and families where relevant.

13. Links with other policies

This policy should be read alongside:

- Child Protection Policy
- Behaviour Policy

- Anti-Bullying Policy
- PSHE and RSE Policy
- ICT and Acceptable Use Policy
- Mobile Phone and Smartwatch Policy
- Staff Code of Conduct and disciplinary procedures
- Data Protection Policy and privacy notices
- Complaints Policy and Procedure
- Supporting Pupils with Medical Conditions Policy.

Appendix 1: Online safety training needs self-audit

Name: _____ Date: _____

Question	Yes / No	Comments / training need
Do you know who has lead responsibility for online safety in school?		
Do you understand the ways children can experience or cause harm online?		
Do you know what to do if a child approaches you with an online safety concern?		
Are you familiar with the acceptable use requirements for your role?		
Do you understand the filtering and monitoring arrangements and your responsibilities?		
Do you know how to report a filtering or monitoring failure?		
Do you understand the school's approach to cyber-bullying and child-on-child online abuse?		
Do you understand the rules for using generative AI and protecting confidential information?		
Do you understand the school's mobile phone-free arrangements?		
Are there any areas of online safety in which you need further training?		

Appendix 2: Online safety incident recording checklist

Field	Record / prompt
Date and time	
Where / how the incident occurred	
Child(ren) / adult(s) involved	
Risk category	Content / Contact / Conduct / Commerce / Technical
Summary of concern or incident	
Immediate safeguarding action	
DSL decision and rationale	
Evidence secured or preserved	
Filtering / monitoring failure involved?	Yes / No - details
External advice or referral	
Parent/carer communication	
Behaviour / anti-bullying action	
Follow-up and review date	
Learning / system change required	