Heatherside Junior School
Online Safety Policy 2026–2027

Approved by Governors: 17th September 2026
Next Review: September 2027

1. Policy Statement

Heatherside Junior School recognises that technology and the internet are an essential part of modern life, learning and communication. We are committed to providing a safe, secure and positive digital environment where pupils, staff, governors, volunteers and visitors can use technology responsibly. The school understands that online safety is a safeguarding issue and is integral to our wider safeguarding responsibilities. Children may be exposed to risks online that are equally, if not more, harmful than those encountered offline. We therefore take a whole-school approach to online safety and digital safeguarding.

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk. The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy.

This policy should be read alongside the school's safeguarding procedures and reflects the requirements of **Keeping Children Safe in Education (KCSIE) 2026**, which states that online safety should be considered a safeguarding issue running through all aspects of school life.

2. Aims

This policy aims to:

- Safeguard and promote the welfare of pupils in the digital environment.
- Protect pupils from harmful or inappropriate online content.
- Educate pupils to become safe, respectful and responsible digital citizens.
- Ensure clear procedures for responding to online safety concerns.
- Promote effective partnerships between school, parents and carers.
- Ensure compliance with statutory safeguarding duties and data protection legislation.
- Support staff in understanding their responsibilities regarding online safety.

3. Scope

This policy applies to pupils, staff, governors, volunteers, contractors, visitors and parents and carers (where digital communication involves the school) including when using:

- School equipment and networks.
- Personal devices used within school.
- Remote learning.

- Online activities that impact the welfare or reputation of pupils or the school.

4. KCSIE Requirements

There are 4 types of online safety risks outlined in KCSIE:

CONTENT: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories.

CONTACT: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

CONDUCT: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including those generated using AI and online bullying.

COMMERCE: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

5. Roles and Responsibilities

Governing Body

The Governing Body will:

- Ensure online safety arrangements are effective.
- Ensure appropriate filtering and monitoring systems are in place.
- Review online safety provision annually.
- Receive regular safeguarding and online safety updates.
- Ensure staff receive appropriate training.
- Monitor compliance with statutory guidance.

Headteacher

The Headteacher will:

- Provide strategic leadership for online safety.
- Ensure policies and procedures are implemented.
- Ensure staff receive appropriate training.
- Ensure adequate resources are available.
- Report significant incidents to governors where appropriate.
- Promote a positive culture of digital safety.

Designated Safeguarding Lead (DSL)

The DSL will:

- Take lead responsibility for online safety safeguarding concerns.
- Manage referrals to relevant agencies.
- Maintain records of online safety incidents.

- Monitor local and national safeguarding trends.
- Deliver or coordinate staff training.
- Support staff dealing with online safety incidents.
- Work with parents and external agencies where required.

Staff

All staff will:

- Read and understand KCSIE Part One annually.
- Follow the school's Acceptable Use Agreement.
- Model safe and professional online behaviour.
- Report concerns immediately to the DSL.
- Teach online safety as appropriate.
- Understand filtering and monitoring systems.
- Maintain appropriate professional boundaries online.

Pupils

Pupils will:

- Use technology responsibly.
- Follow the Acceptable Use Agreement.
- Report concerns to a trusted adult.
- Respect others online.
- Protect their personal information.
- Use school devices and networks appropriately.

Parents and Carers

Parents and carers are encouraged to:

- Support safe internet use at home.
- Monitor age-appropriate use of apps, games and social media.
- Report any concerns affecting pupils' wellbeing or behaviour.
- Attend online safety workshops where available.
- Reinforce school messages about safe online behaviour.

6. Online Safety Education

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education. The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity.
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment.
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content including misinformation and disinformation.
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others.
- Understanding the permanency of all online postings and conversations.
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.
- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- Learning about Artificial Intelligence and how to use this safely and appropriately.
- How the law can help protect against online risks and abuse.

7. Filtering and Monitoring

The school will:

- Maintain age-appropriate filtering systems.
- Monitor internet usage in accordance with DfE guidance.
- Review filtering effectiveness regularly.
- Act upon concerns identified through monitoring.
- Ensure staff understand filtering and monitoring responsibilities.

KCSIE expects governing bodies to ensure appropriate filtering and monitoring systems are in place and regularly reviewed.

8. Managing Online Safety Incidents

Online safety incidents may include but are not limited to: cyberbullying, accessing inappropriate content, online harassment, sharing indecent images, grooming concerns, radicalisation concerns, online fraud/scams, AI misuse, data breaches

All staff must:

1. Secure and preserve evidence where appropriate.
2. Record concerns promptly.
3. Report concerns immediately to the DSL.

4. Follow safeguarding procedures where risk of harm exists.

The school will work with parents and, where required, Hampshire Children's Services, Police and Local safeguarding partners where appropriate.

9. Expected use and procedures

Use of email

Staff and governors should use a school email account for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils should use school approved accounts on the school system for educational purposes.

Staff, governors and pupils must not open emails or attachments from suspect sources and should report their receipt to the Headteacher or Admin Officer.

Visiting online sites and downloads

Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required.

If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

Staff must only use pre-approved systems if creating online content. When working with pupils searching for images should be done through Google Safe Search , Google Advanced Search or a similar application that provides greater safety than a standard search engine.

It is prohibited for any users to:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that would contravene national or school policies for behaviour, conduct and safeguarding.
- Reveal or publicise confidential or proprietary information.
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses.
- Use the school's hardware and Wi-Fi facilities for running a private business.
- Access or interfere in any way with other users' accounts.
- Use software or hardware that has been prohibited by the school.

Only a school device may be used to conduct school business outside of school. The only exception would be where a closed, monitorable system has been set up by the school for use on a personal device.

The school may take action where off-site online behaviour affects the safety and wellbeing of pupils or the school community. Any breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

10. Data Protection and Privacy

The school will:

- Comply with UK GDPR and the Data Protection Act 2018.
- Protect personal information.
- Ensure secure handling of pupil records.
- Promote safe digital practices amongst staff and pupils.

11. Remote and Blended Learning

Where remote learning takes place:

- Approved school platforms will be used.
- Appropriate safeguarding measures will apply.
- Staff will follow school communication protocols.
- Pupils will be taught expectations for safe online behaviour.

12. Responding to Emerging Technologies

The school recognises that technologies continue to evolve.

This includes:

- Artificial Intelligence (AI)
- Generative AI tools
- Social media platforms
- Online gaming environments
- Virtual and immersive technologies

Risk assessments, staff guidance and pupil education will be updated as technology develops.

13. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide

understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Review

This policy will be:

- Reviewed annually.
- Updated following legislative changes.
- Reviewed after any significant online safety incident.
- Monitored through safeguarding audits and governor oversight.

Approved By: Governing Body on 17th September 2026
Policy Review Date: September 2027

Responsible Officer: Headteacher / Designated Safeguarding Lead
Named DSL: Hannah Dunn (update annually as required)

Legal Framework

This policy is informed by:

Statutory Guidance

- Keeping Children Safe in Education (KCSIE) 2026
- Working Together to Safeguard Children (2026)
- Teaching Online Safety in Schools (DfE)
- Relationships Education, Relationships and Sex Education and Health Education Regulations
- Prevent Duty Guidance
- Data Protection Act 2018
- UK GDPR

Related School Policies

This policy should be read alongside:

- Child Protection and Safeguarding Policies
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Acceptable Use Agreements (Staff and Pupils)
- Data Protection Policy
- Privacy Notice
- RSHE Policy
- Mobile Phone Policy
- Whistleblowing Policy
- Prevent Risk Assessment
- Complaints Policy