Rode Heath Primary School

Heath Avenue, Rode Heath, Stoke on Trent, ST7 3RY

Telephone: 01270 314414

E-mail Address: admin@rodeheath.cheshire.sch.uk

Headteacher: Mr J. Frankland

Online Safety Policy

Date created: October 2022

Date reviewed: September 2025

Date of renewal: September 2027

Introduction

Rode Heath Primary School is pleased to offer pupils access to a computer network for the internet and a wide range of computing resources. To gain access to the internet, all pupils must obtain parental/carers' permission. Should a parent/carer prefer that a student does not have internet access, use of the computers is still possible for other work such as word processing and coding. Codes of conduct and permissions are found in the children's reading diaries.

Access to the internet carries with it the danger that children could find and view material that is unsuitable for them or that they could be put at risk from unwanted and inappropriate contacts. This policy seeks to ensure that the internet is used appropriately for learning but with safeguards to protect children from harm.

- This policy will operate in conjunction with other important policies in our school, including our Mobile Phone, Digital Device and Social Media Policy, Behaviour Anti-Bullying and Child-on-Child Abuse Prevention Policy, Data Protection Act 2018, UK General Data Protection Regulation (UK GDPR), RHPS Child Protection and Safeguarding Policy, ICT and Computing Policy, Education for a Connected World, Teaching online safety in school, Sharing nudes and semi-nudes: advice for education settings working with children and young people, Harmful online challenges and online hoaxes, Health and Safety Policy, Equality and Diversity Policy, Complaints Policy, Generative AI: product safety expectations 2025, Online Safety Act 2023 and Statutory guidance for schools and colleges - 'Keeping children safe in education' DfE September 2025.

Aims

- To ensure that children's access to inappropriate sites and locations is restricted.
- To ensure that the use of the internet is for proper purposes related to the teaching, learning and curriculum of this school.
- To protect children from harm and upset that could be caused through access to inappropriate sites, materials, images and contacts.
- To make children aware that there are inappropriate sites that are harmful and which must be avoided in school and at home.
- To encourage children to report immediately any inappropriate sites, materials or contacts that they find on the internet, either at school or at home.
- To raise awareness with older children in school, who are likely to be using computers independently at home of the potential risks and dangers of internet use.

- To ensure GDPR compliance is met and fully adhered to. Any breaches are recorded on the school's software system (GDPRiS).

Guidelines

- Appropriate firewalls are in place and must be enabled at all times on all the school computers. Anti-virus software is also installed and kept up-to-date. The school filter system (Schools Broadband) produces reports which go to the Headteacher who then informs the relevant person about it. It is a robust and appropriate filtering (blocking) website system. Senso is also used to safeguard users by monitoring and filtering (blocking) inappropriate or concerning words, phrases, images or other potential harms and sends reports and screenshots to the Headteacher. Depending on the severity of the incident, the Headteacher can be alerted immediately. "Over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding. This is reviewed annually.

- Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.

- Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything (Meeting digital and technology standards in schools and college, 2022)

- Monitoring and filtering is reviewed annually.

- Staff must not under any circumstances, or at any time, disable- or bypass-firewalls on any school-owned computer.

- Children will be supervised by adults when they are given access to the internet.

- KS2 children have their own log-ins for their computers. If an incident occurs, the child can be identified and the necessary procedures will be followed by a member of Senior Leadership Team (SLT).

- Staff must only use computers for school purposes. School computers used by staff at home or in school must not be modified or used for personal use.

- If children bring digitally stored information into school on pen drive or by other means, staff must check the suitability of the information before it is

played on school IT equipment. As part of the GDPR compliance policies, USBs should be encrypted if used.

- Children must be encouraged to notify staff if they, at any time, come across unsuitable material on a computer or a tablet.

- School staff must notify the Headteacher immediately if they find unsuitable or inappropriate material on a computer or storage device.

- Spot checks and audits will be carried out from time-to-time to ensure that computers are being used appropriately.

- Online safety lessons are taught regularly throughout the school via the ProjectEVOLVE software platform (each half-term as part of the Hearts and Minds Curriculum). This framework covers knowledge, skills, behaviours and attitudes across eight strands of our online lives. The eight strands are:

    - Self-Image and Identity.
    - Online Relationships.
    - Online Reputation.
    - Online Bullying.
    - Managing Online Information.
    - Health, Well-Being and Lifestyle.
    - Privacy and Security.
    - Copyright and Ownership.

- The lessons are all linked to the document: Education for a Connected World from the UK Council for Child Internet Safety.

- School will disseminate advice regarding online safety issues for parents/carers via the school website, School Spider message service and newsletter.

- School governors should be aware of how online safety is taught at school and to robustly evaluate policies and procedures relating to this subject. Regular updates in governor meetings are very important with any breaches of the policy referred to.

- For remote education, all weblinks and videos are checked by the teacher to ensure they are appropriate and also posts are checked and verified too. Parents are informed about how the process works.

- Online safety, and the effectiveness of it, is reviewed regularly in the computing risk assessment document.

Cyber Security

Cyber security is about protecting the devices we all use and the services we access online - both at home and work - from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these

devices and online. Staff need to change passwords regularly and ensure they are strong too. Two-factor authentication passwords are used for sensitive accounts such as CPOMS. They need to be careful which emails they access. If there are any concerns, staff know to report these to the Headteacher and IT support team. USBs, if used, should be encrypted. When at home, staff need up-to-date anti-virus software to minimise the threats. Software updates increase the security of the computer. Children are taught skills on how to protect themselves too in the ProjectEVOLVE scheme of work e.g. making passwords strong.

AI Policy

1. Purpose

This policy outlines how AI technologies are used within our primary school, ensuring they support teaching, learning, and administration while maintaining the safety, fairness, and well-being of our pupils.

2. What Is AI?

Artificial Intelligence (AI) refers to systems that simulate human-like thinking, such as making decisions, recognising patterns, or generating content. Examples include writing assistants, voice recognition tools, and educational chatbots.

3. Principles for AI Use

Our school follows these guiding principles:

- **Safety**: All AI tools used must comply with GDPR, safeguarding policies, and data protection laws.
- **Transparency**: Children and staff will be informed when AI is being used and how it works.
- **Equity**: AI should not reinforce bias or create unfair advantage/disadvantage.
- **Support, not replace**: AI is used to assist learning and teaching, not replace the role of the teacher or pupil voice.

4. AI Use in Practice

For Pupils:

- Age-appropriate AI tools may be used to support English, maths, creativity, or feedback (e.g. spell-checkers, educational apps with adaptive learning).
- Pupils will be guided on how to use AI responsibly.
- AI use is always supervised and approved by a teacher.

For Staff:

- AI may be used to support planning, marking, report writing, or admin tasks.
- Staff are encouraged to critically evaluate AI output for accuracy, bias, and appropriateness.

- No confidential or personal pupil data should be input into public or third-party AI tools without consent and due diligence.

For Administration:

- AI tools (e.g. data analysis or scheduling tools) may be used to improve operational efficiency.
- Procurement of AI technologies will follow school procurement guidelines, including risk and data assessments.

5. Risks and Safeguards

- **Bias**: Staff will be aware of possible bias in AI tools and avoid relying solely on them for judgments about pupils.
- **Misinformation**: Pupils and staff will be taught that AI can produce incorrect or misleading information.
- **Data Protection**: Any AI system used must be GDPR-compliant. Pseudonymisation or anonymisation will be used where possible.

6. Education and Training

- Pupils will receive age-appropriate digital literacy education, including how AI works and how to use it safely and responsibly.
- Staff will receive CPD on AI use in education and guidance on ethical considerations.

7. Monitoring and Review

- AI will be reviewed annually or when significant changes occur.
- Feedback from pupils, staff, and parents will be gathered to ensure AI use remains appropriate and effective.

Social Media Policy

The school recognises and embraces the numerous benefits and opportunities that social media offers. While people are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

Definition of social media

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, X, TikTok Instagram, WhatsApp, Snapchat, Flickr and YouTube.

Employees should:

- Be aware of their online reputation and recognise that their online activity can be seen by others including parents/carers, pupils and colleagues on social media.
- Ensure that any use of social media is carried out in line with this policy and other relevant policies, i.e. those of the employer.
- Be aware that any excessive use of social media in school may result in disciplinary action.
- Be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they are about to post on a social networking site is something that they want pupils, colleagues, other employees, or even future employers, to read or see. If in doubt, don't post it!
- Not to upload any content on to social media sites that is confidential to the school or its staff.
- Not to upload any content on to social media sites that brings the school into disrepute.
- Not to upload any content on to social media sites that is unlawful.
- Ensure live streaming is appropriate and doesn't breach any points in this policy.
- Ensure they have checked the consents document when adding pictures/videos of the children to school's social media accounts and that there is always more than one child on the photograph/video.
- Phones should be locked away whilst on school premises (unless given permission by the Headteacher).

Parental/Carers' requirements include:

- Not using their device for photos or videos during school events.
- Not posting photos, videos or comments that include children at the school.
- Not using social media on their own devices while on school premises.
- Not accessing social media while helping at school or on school visits.
- Phones should be locked away whist on school premises.
- Raising queries, concerns and complaints directly with the school rather than posting them on social media – whether on their own pages, in closed groups (e.g. groups set up for school parents/carers to communicate with each other) or on the school's pages.
- Not posting anything malicious about the school or any member of the school community.
- Ensure live streaming is appropriate and doesn't breach any points in this policy.

Children are required to:

- Not join any social networking sites if they are below the permitted age (13 or older for most sites including Facebook and Instagram).
- Tell their parents/carers if they are using the sites, and when they are online.
- Be aware how to report abuse and inappropriate content.
- Not to access social media on school devices, or on their own devices while they're at school.
- Not to make inappropriate comments (including in private messages) about the school, teachers or other children.
- Be aware of the potential problems with live streaming and how to ensure their own safety.
- With potential unlimited access to data on mobile phones etc., children need to be aware of how to keep safe from dangers and to limit screen time.
- Be aware of their digital footprint because information about their online activity can be stored.
- Ensure live streaming is appropriate and doesn't breach any points in this policy.
- In Upper Key Stage 2, if children are walking to and from school, without an adult, they are allowed to bring their mobile phone to school. As soon as they enter the classroom in the morning, the phone must be switched off and handed to the teacher. The teacher will then put the phones in a secure place that cannot be accessed by children throughout the day. The phones are then returned to the children at the end of the day and they are allowed to switch them on as soon as they leave the school premises.

Safeguarding

The use of social networking sites introduces a range of potential safeguarding risks to children and young people.

Potential risks can include, but are not limited to:

- Online bullying.
- Grooming, exploitation or stalking.
- Exposure to inappropriate material or hateful language.
- Encouraging violent behaviour, self-harm or risk taking.

The breadth of issues classified within online safety is considerable and ever evolving. The 'Keeping children safe in education' DfE September 2024 outlines these four important areas of risk to consider:

- content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- contact: being subjected to harmful online interaction with other users; 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 (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- commerce: - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group: https://apwg.org/.

Reporting safeguarding concerns

- Any content or online activity which raises a safeguarding concern must be reported to the lead safeguarding officer in the school and recorded on CPOMS – Safeguarding Software for Schools.
- Any online concerns should be reported as soon as identified as urgent steps may need to be taken to support the child.
- Personal safeguarding issues i.e. harassment or abuse received online while using work accounts should be reported immediately to the Designated Safeguarding Lead (DSL).

Potential and actual breaches of the code of conduct

In instances where there has been a breach of the code of conduct as outlined in this policy, the following will apply:

Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy, this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

Conclusion

Children and staff will be able to enjoy and use the school computers and tablets to:
- Enhance teaching and learning.
- Access useful educational information and materials, without risk of harm or upset.