ROSEMARY WORKS SCHOOL

E-Safety Policy

Including Acceptable Use Policy

Reviewed by Amanda Parker
June 2025

Introduction and Aims

We recognise the link between E-Safety, Safeguarding and Anti-Bullying, so this policy should be read in conjunction with those policies.

New technology is integral to the lives of children and young people in today's society. The internet and other digital and information technologies are tools that open up a world of learning and communication. However, the online world has its own set of challenges.

We recognise the importance of safeguarding children from potentially harmful and inappropriate online material, and we understand that technology is a significant component in many safeguarding and wellbeing issues. Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Keep any personal data and information secure
- Educate children to use the internet purposefully, keeping themselves safe when using the internet

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as 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 – personal online behaviour that increases the likelihood of, or causes, harm, such as 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
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Managing access and security

The school provides managed internet access to its staff and pupils in order to enhance the education provided by the school and help pupils to learn how to assess and manage online risks, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

The school ensures that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is functioning and effective.

The school ensures that its equipment has adequate security and protection. Access to school networks is controlled by passwords and additional authentication. Different types of users have access to different parts of the school systems depending on their roles. As with all online systems, passwords should be unique, suitably complex and changed regularly.

Systems are in place to ensure that school internet use can be monitored and logged so if there are any incidents, the school can receive alerts and identify patterns of behaviour and inform e-safety policy.

Pupils' access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.

Filtering and Monitoring

The school uses a highly regarded filtering system, Securly, to filter access to the internet. This is accredited by the UK Safer Internet Centre. Securly has different restrictions for different groups of users, with tighter restrictions for pupils. The DSL receives instant alerts when a site is blocked.

The school uses Aware, provided by Securly, to monitor internet use beyond what is blocked. Aware monitors internet use for signs of bullying, self harm, suicide or violence and sends an instant notification to the DSL if concerning words or phrases are used.

These tools are tested termly by the DSL for their effectiveness, using testfiltering.com, provided by the UK Safer Internet Centre. This checks that the following categories of content are fully blocked:

- Child Sexual Abuse Material (websites on the IWF Child Abuse Control URL list)
- Terrorism Content (websites on the Counter-Terrorism Internet Referral Unit list)
- Adult Content (pornography)
- Offensive language

E-Safety Lessons

The school incorporates age-appropriate e-safety lessons into the wider school curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. This includes Life Learning Lessons and in the computing curriculum, as well as assemblies and participation in events such as Safer Internet Day.

Pupils are also advised about current online risks, peer pressure, smartphone use, websites, online games and social media trends. They are advised never to share passwords, or give out personal details or information which may identify them or their location.

E-mail

Staff may only use school provided email accounts for communication or access to the school systems. Staff to parent email communication must only originate from a school email address. Any group emails sent to parents are sent using the school's email groups provided for this purpose. Pupils are not given any access to the school email service, but have a school provided login to access Chromebooks, Google Classroom and other online apps.

Any unexpected incoming email should be treated as suspicious and attachments not opened, or links clicked. Even if the author is known, any email attachments still may potentially be suspicious if its receipt was not expected or there are any doubts about the veracity of the email. Emails containing links which prompt you to login to access should especially be treated with suspicion. If in any doubt contact the IT department for advice.

Publishing content

The contact details for published content e.g. the school website, or any other externally visible media will always be the school address, email and telephone number.

Permission will be obtained from parents or carers before photographs or names of pupils are published on the school website, prospectus, newsletter or social media. Parents provide this consent during the admissions process, and may be reaffirmed from time to time if circumstances change.

Any content which contains any excerpts or other content originating from a third party should always be checked for permission before being reused.

Data Storage

Any school data and files should only ever be stored and accessed via the school provided, cloud based or local systems (i.e. school Google Drive accounts or the school server). Local (offline) storage of any confidential data (e.g. containing names of pupils) on computers on laptops is only ever permitted on school owned equipment. If confidential attachments are inadvertently downloaded locally by opening attachments or generating reports, for example, they must always be deleted immediately after use. Use of any other online systems not sanctioned by the school to store any confidential data is prohibited.

Sharing confidential files or data externally must always be using approved methods and with the permission of the senior leadership team.

Software Usage

Generally, most software used at school is cloud-based (accessed via the internet). There are a few exceptions used in the classroom, such as software designed for use with specific hardware, for example interactive white boards, or Microsoft Office products.

Although we are always exploring new software products and services for use at school, use of any software which is not currently licenced and approved by the school is not permitted.

No software should ever be installed on a computer or app downloaded on school equipment without prior approval from the school.

Staff should not start trials of new software services without prior approval from the Senior Leadership.

Use of social media

Staff:

School staff's social media profiles should not be available to pupils. Staff should consider using an alternative name, such as first and middle name instead of full names, and set personal profiles to private. Staff who use public social media for professional purposes, e.g. for their own small businesses, must ensure that this is kept separate to personal profiles. Staff should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their position as a member of the school community. This includes activity on private social media accounts.

Staff should not attempt to contact pupils or their parents via social media, or any other means outside school, in order to develop any sort of relationship. They will not make any efforts to find pupils', former pupils' or parents' social media profiles.

The school admin and marketing team uses social media for marketing purposes, accessing this from school owned and managed devices.

Pupils:

While primary-aged pupils are below the minimum age for most social media platforms, and these are blocked on school systems, we recognise that some children may still access and use social media outside of school. We are committed to supporting pupils and families to navigate this safely and responsibly, in line with our Safeguarding and Anti-Bullying policies.

We teach pupils about the risks associated with social media use, including inappropriate content, contact from strangers, privacy concerns, misinformation and online bullying. Pupils are encouraged to speak to a trusted adult if they encounter anything online that upsets or worries them, whether in school or at home.

If the school becomes aware that a pupil is using social media, even where no immediate safeguarding or bullying concern is identified, we will work sensitively with the pupil and their parents to offer guidance, reinforce online safety education, and encourage responsible and age-appropriate use. This may include signposting parents to resources to help set boundaries and support their child's online behaviour.

Any incidents of online bullying or harmful behaviour between pupils, whether occurring on school premises or outside of school hours, will be taken seriously and investigated in line with our Anti-Bullying and Safeguarding policies. Such behaviour may result in appropriate pastoral support, sanctions, and parental involvement to ensure the wellbeing of all children involved.

We work closely with parents and carers to raise awareness of age-appropriate online use, promote open communication at home, and support families in setting boundaries around social media.

Use of mobile phones and smart technology

Pupils:

Pupils are not permitted to have mobile phones, tablets or connected smart watches or cameras at school or on trips. If in the rare event of a parent wishing for his/her child to bring a mobile phone to school to contact the parent after school:

- the parent must put their request in writing to the Head Teacher
- the phone must be handed in, switched off, to the school office first thing in the morning and collected from the office by the child at home time.

Mobile phones, tablets, smartwatches or cameras brought to school by pupils without permission will be confiscated and must be collected by the parent.

Staff:

- Staff may use the school mobile phones to take photographs of children for communication, recording or marketing purposes. This is fully secure and managed by school systems.
- A school mobile will be carried to sporting fixtures away from school, on educational visits and residentials for contacting the school or parents in the event of an emergency.
- Staff must have their personal phones on silent or switched off during class time. Phones must be kept out of sight (e.g. drawer or handbag) when staff are with children. Personal tablets or connected smart watches (e.g. with internet access or camera abilities) must also be kept out of sight when with children.
- Staff working in the EYFS, including in wrap around care or lunchtime supervision, may not have their personal devices with them in the room with children. Mobile phone lockers are provided for staff in the office.
- Use of phones/devices must be limited to PPA or break times when no children are present in areas of the school where there is no access for children. Calls/ texts must be made/received in private during PPA or break time. Personal phones must not be used to photograph children, contact parents or share school data.
- Staff must be aware that the web filters in place in the school do not apply to mobile data from personal mobile phones, so these are for personal use only and must not be used with the pupils. This includes devices tethered to personal mobile hotspots.
- Staff requiring the use of personal devices that can connect to the internet must seek permission from the Head Teacher in advance of this. The Head Teacher will conduct a Risk Assessment and the staff member will sign an agreement stating the measures they will take to reduce any risk (e.g. turning off the internet and notifications, covering the camera.)
- Personal devices will only be used near children in case of emergency or when it would be more harmful not to, e.g. during an emergency lockdown.

Parents:

- Parents are not permitted to use their mobile phones on the school premises, including to take photographs of children. The school exercises the right to view and request deletion of any unauthorised photograph taken using a mobile device.
- Parents needing to make an urgent call will be asked to wait outside or in an area away from children until they are able to put their mobile phones away.
- For the purpose of recording class assemblies, sports days and other public performances or appearances, parents may take photos of their children. The school will record and share performances, so parents are encouraged not to do so. Parents are not permitted under any circumstance to distribute photographs or videos of aforementioned events over the internet, social media or messaging apps.

Artificial Intelligence

AI technologies are increasingly present in everyday life, from predictive text and recommendation systems to more advanced tools such as chatbots and content generators. At Rosemary Works, we recognise both the opportunities and risks that AI brings, and we aim to prepare pupils to engage with these tools safely, ethically, and critically.

We teach children to:

- Recognise when they are interacting with AI or automated systems.
- Understand that AI-generated information may be inaccurate, biased, or inappropriate.
- Apply critical thinking when evaluating information, whether from AI, search engines, or other sources.
- Never share personal information with AI tools or online platforms without adult supervision.

Pupils are not currently permitted to use generative AI tools (such as chatbots or image generators), as these are not considered developmentally appropriate.

Staff remain responsible for modelling safe and responsible use of AI, and any concerns arising from AI-related activity should be reported to the DSL in line with our safeguarding and e-safety procedures.

Please see our Artificial Intelligence Policy for further detail.

Assessing risks and reporting

While the school will take all reasonable precautions to prevent access to any inappropriate or unsuitable material, due to the world-wide scale and ever-changing, linked internet content, it is not possible to guarantee 100% that any unsuitable material will never appear on a school computer or another device whilst on the school premises.

Any such incident must be reported to the Safeguarding Lead for further action, and followed up by the IT department to ensure the risk is blocked or mitigated. Furthermore, all staff must contact the Safeguarding Lead if they suspect any student or staff member is using technology inappropriately, e.g. grooming, accessing age-inappropriate materials, or involved in possible radicalisation activities falling under our Prevent Duty. In all cases or if in any

doubt, please contact the Designated Safeguarding Lead – See Safeguarding and Child Protection Policy.

Online Abuse

Staff and parents should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non- consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Please see the Safeguarding policy for further detail.

Handling e-safety complaints

Complaints of internet misuse by students will be dealt with according to the school's behaviour policy.

Complaints of a Safeguarding nature must be dealt with in accordance with the school's safeguarding and child protection procedures. In the first instance the Safeguarding Lead must always be contacted.

Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behaviour policy.

Acceptable Use Policy

This e-Safety policy should be treated in conjunction with the Acceptable Use Policy (see appendices).

Staff, visitors and volunteers must agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet. Pupils' access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.

All school staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet at school.

Review

This policy will be reviewed by the Head Teacher or Head of IT every two years.

Further Information and Resources

There is a wealth of information available to support schools and parents to keep children safe online. The following is not exhaustive but should provide a useful starting point:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.pshe-association.org.uk

www.educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

https://www.ceop.police.uk/safety-centre/

http://www.cscb-new.co.uk/?page_id=95

Appendix 1: Acceptable Use Policy and Agreement
for staff, governors, volunteers and visitors

When using the school's ICT facilities and accessing the internet in school, or outside school on a school device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote any private business, unless that business is directly related to the school, without explicit written consent from the Head Teacher

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems, including personal devices using the school's wifi.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

I will not access personal social networking accounts or use personal devices in school in front of children or in a way that interferes with work duties, or use any personal device to photograph children. I will not use personal email, social or telephone accounts to communicate with parents or students. I will maintain professional boundaries on personal social media, not posting anything that could reflect negatively on the school or its staff.

Signed: Print name:

Date: