



Rawmarsh Ryecroft Infant School

Online Safety Policy

Last Updated: October 2025

Review Date: October 2027

Contents:

Statement of intent

1. Legal Framework
2. Roles and Responsibilities
3. The Curriculum
4. Staff Training
5. Educating Parents
6. Classroom Use
7. Internet Access
8. Filtering and Monitoring Online Activity
9. Network Security
10. Emails
11. Online hoaxes and harmful online challenges
12. The School Website
13. Use of School-owned Devices
14. Managing reports of online safety incidents
15. Responding to specific online safety concerns
16. Remote learning

Statement of Intent

Rawmarsh Ryecroft Infant School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- | | |
|-----------------|---|
| Content: | Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views. |
| Contact: | Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults. |
| Conduct: | Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying. |

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2020'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World - 2020 edition'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Acceptable Use Agreement
- Data and E-Security Breach Prevention and Management Plan
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy
- RSE and Health Education Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Photography Policy
- Device User Agreement
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy
- Pupil Remote Learning Policy

2. Roles and Responsibilities

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher is responsible for:

- Supporting the Designated Safeguard Lead and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Keeping parents up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the Designated Safeguard Lead and governing board to update this policy on an annual basis.

The Designated Safeguard Lead is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.
- Reporting to the governing board about online safety on an annual basis.
- Working with the headteacher and governing board to update this policy on an annual basis.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to this policy, the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online

3. The Curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- Relationships and Health Education
- PSHE
- Computing

The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

Online safety teaching is always appropriate to pupils' ages and developmental stages.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks pupils may face online are always considered when developing the curriculum.

The Designated Safeguard Lead is involved with the development of the school's online safety curriculum.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO, work to ensure the curriculum is tailored so these pupils receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?
-

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The Designated Safeguarding Lead advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

1. Staff Training

All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

Online safety training for staff is updated annually and they also receive regular online safety updates as required and at least annually.

The Designated Safeguard Lead and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

The Designated Safeguard Lead acts as the first point of contact for staff requiring advice about online safety.

2. Educating Parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home.

Parents are provided with information about the school's approach to online safety and their role in protecting their children.

Parents are sent a copy of the Acceptable Use Agreement and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

3. Classroom Use

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.

Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time - this supervision is suitable to their age and ability.

4. Internet Access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

5. Educating Parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home.

Parents are provided with information about the school's approach to online safety and their role in protecting their children.

Parents are sent a copy of the Acceptable Use Agreement and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

6. Classroom Use

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.

Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

7. Filtering and Monitoring Online Activity

- The governing board ensures the school's ICT network has appropriate filters and monitoring systems in place.
- The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.
- The ICT technicians ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- ICT technicians undertake checks on the filtering and monitoring systems to ensure they are effective and appropriate.
- Requests regarding making changes to the filtering system are directed to the headteacher.
- Any changes made to the system are recorded by ICT technicians.
- Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.
- Deliberate breaches of the filtering system are reported to the Designated Safeguard Lead and ICT technicians, who will escalate the matter appropriately.
- If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy.
- If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Staff Conduct Policy.
- The school's network and school-owned devices are appropriately monitored.
- All users of the network and school-owned devices are informed about how and why they are monitored.

8. Network security

- Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians.
- Firewalls are switched on at all times.
- ICT technicians review the firewalls on a monthly basis to ensure they are running correctly, and to carry out any required updates.
- Staff are advised not to download unapproved software or open unfamiliar email attachments.
- Staff members report all malware and virus attacks to ICT technicians.
- All members of staff have their own unique usernames and private passwords to access the school's systems.
- Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.
- Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.

- Users are required to lock access to devices and systems when they are not in use.
- Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details.
- If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.
- Full details of the school's network security measures can be found in the Data and E-Security Breach Prevention Policy.

9. Emails

- Access to and the use of emails is managed in line with the Data Protection Policy and Acceptable Use Agreement.
- Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement.
- Personal email accounts are not permitted to be used on the school site.
- Any email that contains sensitive or personal information is only sent using secure and encrypted email.
- The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this.
- Chain letters, spam and all other emails from unknown sources are deleted without being opened.
- Any cyberattacks initiated through emails are managed in line with the Data and E-Security Breach Prevention Policy.

10. Online hoaxes and harmful online challenges

For the purposes of this policy, an **“online hoax”** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **“harmful online challenges”** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

The Designated Safeguard Lead ensures that pupils are taught about how to critically identify when online content is untrue or harmful and how to respond to this content, in line with [section 3](#) of this policy.

The Designated Safeguard Lead will work with the SENCO to assess whether some pupils, e.g. pupils who have been identified as being vulnerable or pupils with SEND,

need additional help with identifying harmful online challenges and hoaxes, and tailor support accordingly.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the Designated Safeguard Lead immediately.

The Designated Safeguard Lead will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country.

Where the harmful content is prevalent mainly in the local area, the Designated Safeguard Lead will consult with the Local Authority about whether quick local action can prevent the hoax or challenge from spreading more widely.

The Designated Safeguard Lead will check the factual basis of harmful online challenges or hoaxes against a known, reliable and trustworthy source, e.g. the UK Safer Internet Centre, and will carefully consider if a challenge or story is a hoax or is harmful prior to providing any direct warnings to pupils or parents.

The school understands that discussing or naming a specific online hoax can, in some cases, needlessly increase pupils' exposure to distressing content, and will avoid showing pupils distressing content where doing so is not considered absolutely necessary for preventing its spread or easing fears amongst the school community.

Where the Designated Safeguard Lead's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed with the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The Designated Safeguard Lead will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Prior to deciding how to respond to a harmful online challenge or hoax, the Designated Safeguard Lead will decide whether each proposed response is:

- Factual and avoids needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils that is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.

- Age-appropriate and appropriate for the relevant pupils' developmental stage.
- Supportive.

11. The School Website

- The headteacher is responsible for the overall content of the school website - they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.
- The website complies with guidelines for publications including accessibility, data protection, and respect for intellectual property rights, privacy policies and copyright law.
- Personal information relating to staff and pupils is not published on the website.
- Images and videos are only posted on the website if appropriate and with prior approval.

12. Use of School-Owned Devices

- Staff members are issued with a laptop to assist with their work.
- Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.
- School-owned devices are used in accordance with the Device User Agreement.
- Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.
- All school-owned devices are password protected.
- All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.
- No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.
- Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with relevant policies.

13. Managing Reports of Online Safety Incidents

Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

Concerns regarding a pupil's online behaviour are reported to the DSL who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians. Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The Designated Safeguard Lead will decide in which cases this response is

appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSL.

14. Responding to specific online safety concerns

Cyberbullying

- Cyberbullying, against both pupils and staff, is not tolerated.
- Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

Online sexual violence and sexual harassment between children (peer-on-peer abuse)

- The school recognises that peer-on-peer abuse can take place online.
- The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.
- Concerns regarding online peer-on-peer abuse are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.

Sexting and the sharing of indecent imagery of pupils

Sharing indecent imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.

Staff will receive appropriate training regarding child sexual development and will understand the difference between sexual behaviour that is considered normal and developmentally expected, and sexual behaviour that is inappropriate and/or harmful. All concerns regarding sexting are reported to the Designated Safeguard Lead.

The DSL will use their professional judgement, in line with the Child Protection and Safeguarding Policy, to determine whether the incident is **experimental**, i.e. expected for the developmental stage of the pupils involved, or **aggravated**, i.e. involves additional or abusive elements, the images are used recklessly or there is an intent to harm the pupil depicted.

Where the incident is categorised as 'experimental', the pupils involved are supported to understand the implications of sharing indecent imagery and to move forward from the incident.

Where there is reason to believe the incident will cause harm to the pupil depicted, or where the incident is classified as 'aggravated', the following process is followed:

- The DSL holds an initial review meeting with appropriate school staff
- Subsequent interviews are held with the pupils involved, if appropriate
- Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm

- At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
- The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented

When investigating a report, staff members will not view any nude and semi-nude images unless there is a good and clear reason to do so. If a staff member believes there is a good reason to view nude or semi-nude imagery as part of an investigation, they discuss this with the Designated Safeguard Lead first. The decision to view imagery is based on the professional judgement of the DSL and always complies with the Child Protection and Safeguarding Policy.

If a decision is made to view the imagery, the Designated Safeguard Lead will be satisfied that viewing:

- Is the only way to make a decision about whether to involve other agencies because it is not possible to establish the facts from any pupil involved.
- Is necessary in order to report the image to a website or suitable reporting agency to have the image taken down, or to support the pupil in taking down the image or in making a report.
- Is unavoidable because a pupil has presented it directly to a staff member or nudes or semi-nudes have been found on an education setting's device or network.

Where it is necessary to view the imagery the Designated Safeguard Lead will:

- Never copy, print, share, store or save images; this is illegal.
- Undertake the viewing themselves, or make sure viewing is undertaken by another member of the safeguarding team.
- Make sure viewing takes place with another member of the SLT in the room; additional people in the room will not view the imagery.
- Only view the imagery on the school premises.
- Record how and why the decision was made to view the imagery.
- Make sure that images are viewed by a member of staff of the same sex as the pupil, where appropriate.
- Ensure that, if devices need to be passed on to the police, the device is confiscated, disconnected from Wi-Fi and data and turned off immediately to avoid imagery being accessed remotely; the device will be secured until it can be collected by police.

Imagery will not be purposefully viewed where it will cause significant harm or distress to any pupil involved, in line with the Designated Safeguard Lead's professional judgement.

Any accidental or intentional viewing of imagery that is undertaken as part of an investigation is recorded.

Where a staff member has accidentally viewed a nude or semi-nude image, the Designated Safeguard Lead will ensure they are provided with the appropriate support, as viewing nude or semi-nude imagery of pupils can be distressing.

Online abuse and exploitation

- Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.
- The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.
- All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the Designated Safeguard Lead.

Online hate

- The school does not tolerate online hate content directed towards or posted by members of the school community.
- Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved.

Online radicalisation and extremism

- The school's filtering system protects pupils and staff from viewing extremist content.
- Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Child Protection and Safeguarding Policy and Prevent Duty Policy.

15. Remote learning

All remote learning is delivered in line with the school's Remote Learning Policy.

All staff and pupils using video communication must:

- Communicate in groups - one-to-one sessions are only carried out where necessary.
- Wear suitable clothing - this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background - 'private' living areas within the home, such as bedrooms, are not permitted during video communication.

- Use appropriate language - this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the SENCO.

Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

