

# RED ROSE SCHOOL

## ON-LINE SAFETY POLICY

Section 7

2a

Updated: January 2025

Next review: January 2026

### Contents:

#### Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Managing online safety](#)
4. [Cyberbullying](#)
5. [Peer-on-peer sexual abuse and harassment](#)
6. [Grooming and exploitation](#)
7. [Mental health](#)
8. [Online hoaxes and harmful online challenges](#)
9. [Cyber-crime](#)
10. [Online safety training for staff](#)
11. [Online safety and the curriculum](#)
12. [Use of technology in the classroom](#)
13. [Use of smart technology](#)
14. [Educating parents](#)
15. [Internet access](#)
16. [Filtering and monitoring online activity](#)
17. [Network security](#)
18. [Emails](#)
19. [Generative Artificial Intelligence \(AI\)](#)
20. [Social networking](#)
21. [The school website](#)
22. [Use of devices](#)
23. [Remote learning](#)
24. [Monitoring and review](#)

#### Appendices

- A. [Online harms and risks – curriculum coverage](#)

## Statement of intent

Red Rose 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 four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

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.

Mrs Gill Makinson      Head Teacher      January 2025

## **1. Legal framework**

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2024) 'Keeping children safe in education'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

This policy operates in conjunction with the following school policies including:

- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- RSE and Health Education Policy
- Searching, Screening and Confiscation Policy
- Pupils' Personal Electronic Devices Policy
- Staff Code of Conduct
- Cyber Security Policy
- Behaviour Policy
- Data Protection Policy
- Confidentiality Policy
- Photography Policy
- Staff ICT and Electronic Devices Policy
- Pupil Remote Learning Policy

## **2. Roles and responsibilities**

The Head Teacher is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Ensuring all staff undergo safeguarding and child protection training, including online safety.
- 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.

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the deputy DSL 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 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 informed about current online safety issues regarding how the school is keeping pupils safe.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school in liaison with the ICT Technician.
- Understanding 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.
- 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 updated with current research, legislation and online trends.
- Ensuring all members of the school community understand the reporting procedure for online safety incidents and inappropriate internet use, both by pupils and staff.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Identify trends and any gaps in the school's provision, and using this data to update the school's procedures.

ICT technician is 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 Head Teacher.
- 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.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.

- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Adhering to 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.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

### **3. Managing online safety**

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Head Teacher has overall responsibility for the school's approach to online safety and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular training
- Online safety is integrated into learning throughout the curriculum and in PSHE
- Assemblies are conducted on the topic of remaining safe online

#### **Handling online safety concerns**

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour are reported to the Head Teacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the Head Teacher, it is reported to the Proprietor.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Head Teacher and ICT technician, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Head Teacher 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 DSL 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.

## **4. Cyberbullying**

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

## **5. Child-on-Child sexual abuse and harassment**

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of school, off and online, and remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is

created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking “sides”, often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment.

Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

## **6. Grooming and exploitation**

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer’s attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel ‘special’, particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.

- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

### **Child sexual exploitation (CSE) and child criminal exploitation (CCE)**

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

### **Radicalisation**

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

## **7. Mental health**

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

## **8. 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.

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 DSL immediately.

The DSL 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.

Prior to deciding how to respond to a harmful online challenge or hoax, the Head Teacher/DSL will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge e.g. where content is explained to younger pupils but 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.
- Appropriate for the relevant pupils’ age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

The Head Teacher/DSL 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.

## **9. Cyber-crime**

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and ‘booting’, which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The Head Teacher/DSL will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

In addition, the school will implement a cyber awareness plan for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cyber crime.

The school will implement its cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges' and the Cyber Security Policy.

## **10. Online safety training for staff**

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

## **11. Online safety and the curriculum**

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

- PSHE & Citizenship (including RSE)
- ICT

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

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

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in [Appendix A](#) of this policy.

The Head Teacher/DSL is involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

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

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

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?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils including are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Head Teacher/ DSL decides when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher considers 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. Lessons and activities are planned carefully so they do not draw attention to a pupil who is or has been abused or harmed online.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

## **12. Use of technology in the classroom**

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

- Computers
- Laptops
- Tablets
- Device cameras

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.

### **13. Use of smart technology**

While the school recognises that the use of smart technology can have educational benefits, there are also associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's technology Acceptable Use for Pupils.

Staff will use all smart technology and personal technology in line with the school's Staff ICT and Electronic Devices Policy.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks may cause them to use the internet in a way which breaches the school's acceptable use of ICT agreement.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the school.

Where necessary, the school will ban pupils from bringing personal technology on the school site.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept updated with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

### **14. Educating parents**

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

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- baseline age for social media platforms
- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

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.

## **15. Internet access**

Pupils, staff and other members of the school community need to read and sign the Acceptable Use Agreement agreeing to the conditions of use of school internet access.

All staff 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.

## **16. Filtering and monitoring online activity**

The school has appropriate filters and monitoring systems in place and that it is meeting the DfE's '[Filtering and monitoring standards for schools and colleges](#)'.

The Head Teacher ensures the school's ICT network has appropriate filters and monitoring systems in place and that 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Head Teacher and ICT technician determine what filtering and monitoring systems are required. 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 technician undertakes regular 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 Head Teacher. Any changes made to the system are recorded by ICT technician. Reports of inappropriate websites or materials are made to the ICT technician immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the Head Teacher and the ICT technician. 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, this will be dealt with in line with the Staff Handbook.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

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. Concerns identified through monitoring are reported to the Head Teacher/DSL who manages the situation in line with the Child Protection and Safeguarding Policy.

## **17. Network security**

Technical security features, such as anti-virus software, are kept up-to-date and managed by the ICT technician. The ICT technician reviews the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments and are expected to report all malware and virus attacks to the ICT technician.

All members of staff have their own unique school usernames and private passwords to access the school's systems. Pupils in class, year or key stage and above are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private.

Users inform the headteacher or ICT technician if they forget their login details, who will arrange for the user to re access the systems. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Head Teacher is informed and decides the necessary action to take.

Users are required to lock access to devices and systems when they are not in use.

## **18. Emails**

Access to and the use of emails is managed in line with the Data Protection Policy, and Acceptable Use Agreement.

Staff and pupils are given approved school email accounts and use these accounts at school and when doing school-related work outside of school hours. Staff and pupils must agree to and sign the Acceptable Use Agreement.

Personal email accounts are not permitted to be used for any school-related matters. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and pupils are required to block spam and junk mail, and report the matter to the ICT technician. 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 cyber-attacks initiated through emails are managed in line with the Data and Cyber-security Policy and Plan.

## **19. Generative Artificial Intelligence (AI)**

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

The school will prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

## **20. Social networking**

### **Personal use**

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson/ PPA time. Staff may use personal social media during their break and lunchtimes away from the school site or in the staff room; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

The Staff Handbook provides guidance on safe and responsible use of social media. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

Where staff have an existing personal relationship with a parent or pupil, and already connected with them on social media, e.g. they are friends with a parent at the school; they will disclose this to the DSL and Head Teacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

## **21. The school website**

The Head Teacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, updated and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, 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 the provisions in the Photography Policy are met.

## **22. Use of devices**

### **School-owned devices**

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Staff ICT and Electronic Devices Policy and Pupils' Personal Electronic Devices Policy.

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablet or laptop to use during lessons.

School-owned devices are used in accordance with the device User Agreement. All school-owned devices are password protected. 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.

The ICT technician reviews all school-owned devices to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technician.

Staff members or pupils found to be misusing school-owned devices will be managed in line with the appropriate Policy or Code of Conduct.

### **Personal devices**

Personal devices are used in accordance with the Staff ICT and Electronic Devices Policy and the Pupils' Personal Electronic Devices Policy. Any personal electronic device that is brought into school is the responsibility of the user.

Pupils are not permitted to have on their person or access their personal devices in school. Personal devices are handed in to the class staff at the start of the school day and returned at the end of the day. If a pupil needs to contact their parents during the school day, they may use the phone in the school office.

Where a pupil needs an accessibility feature on a personal device to help them access education, e.g. where a pupil who is deaf uses their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are managed on a case-by-case basis.

Pupils' devices can be searched, screened and confiscated in accordance with the Searching, Screening and Confiscation Policy. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.



## **23. Remote learning**

All remote learning is delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

## **24. Monitoring and review**

The school recognises that the online world is constantly changing; therefore the ICT technician and the Head Teacher /DSL conduct light-touch reviews of this policy to evaluate its effectiveness.

The Head Teacher/DSL reviews this policy in full on an annual basis and following any online safety incidents.

Any changes made to this policy are communicated to all members of the school community.

## Appendix A: Online harms and risks – curriculum coverage

[The table below contains information from the DfE’s ‘Teaching online safety in schools’ guidance about what areas of online risk schools should teach pupils about.]

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
<b>How to navigate the internet and manage information</b>		
Age restrictions	<p>Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● That age verification exists and why some online platforms ask users to verify their age</li> <li>● Why age restrictions exist</li> <li>● That content that requires age verification can be damaging to under-age consumers</li> <li>● What the age of digital consent is (13 for most platforms) and why it is important</li> </ul>	<p>This risk or harm is covered in the following curriculum areas as appropriate:</p> <ul style="list-style-type: none"> <li>● PSHE</li> <li>● Health education</li> <li>● Computing</li> </ul>
How content can be used and shared	<p>Knowing what happens to information, comments or images that are put online. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● What a digital footprint is, how it develops and how it can affect pupils’ futures</li> <li>● How cookies work</li> <li>● How content can be shared, tagged and traced</li> <li>● How difficult it is to remove something once it has been shared online</li> <li>● What is illegal online, e.g. youth-produced sexual imagery (sexting)</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● PSHE</li> <li>● <b>or</b> RSE</li> <li>● Health education</li> <li>● Computing</li> </ul>
Disinformation, misinformation and hoaxes	<p>Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● Disinformation and why individuals or groups choose to share false information in order to deliberately deceive</li> <li>● Misinformation and being aware that false and misleading information can be shared inadvertently</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● PSHE</li> <li>● <b>or</b> RSE</li> <li>● Health education</li> <li>● Computing</li> </ul>

	<ul style="list-style-type: none"> <li>● Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons</li> <li>● That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online</li> <li>● How to measure and check authenticity online</li> <li>● The potential consequences of sharing information that may not be true</li> </ul>	<ul style="list-style-type: none"> <li>● Citizenship</li> </ul>
Fake websites and scam emails	<p>Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● How to recognise fake URLs and websites</li> <li>● What secure markings on websites are and how to assess the sources of emails</li> <li>● The risks of entering information to a website which is not secure</li> <li>● What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email</li> <li>● Who pupils should go to for support</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● PSHE</li> <li>● <b>or</b> RSE</li> <li>● Health education</li> <li>● Computing</li> </ul>
Online fraud	<p>Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● What identity fraud, scams and phishing are</li> <li>● That children are sometimes targeted to access adults' data</li> <li>● What 'good' companies will and will not do when it comes to personal details</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● PSHE</li> <li>● <b>or</b> RSE</li> <li>● Health education</li> <li>● Computing</li> </ul>
Password phishing	<p>Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following:</p>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● PSHE</li> </ul>

	<ul style="list-style-type: none"> <li>● Why passwords are important, how to keep them safe and that others might try to get people to reveal them</li> <li>● How to recognise phishing scams</li> <li>● The importance of online security to protect against viruses that are designed to gain access to password information</li> <li>● What to do when a password is compromised or thought to be compromised</li> </ul>	<ul style="list-style-type: none"> <li>● Computing</li> </ul>
Personal data	<p>Online platforms and search engines gather personal data – this is often referred to as ‘harvesting’ or ‘farming’. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● How cookies work</li> <li>● How data is farmed from sources which look neutral</li> <li>● How and why personal data is shared by online companies</li> <li>● How pupils can protect themselves and that acting quickly is essential when something happens</li> <li>● The rights children have with regards to their data</li> <li>● How to limit the data companies can gather</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● PSHE</li> <li>● or RSE</li> <li>● Computing</li> </ul>
Persuasive design	<p>Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible</li> <li>● How notifications are used to pull users back online</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● Health education</li> <li>● Computing</li> </ul>
Privacy settings	<p>Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● How to find information about privacy settings on various devices and platforms</li> <li>● That privacy settings have limitations</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● PSHE</li> <li>● or RSE</li> <li>● Health education</li> </ul>

		<ul style="list-style-type: none"> <li>• Computing</li> </ul>
Targeting of online content	<p>Much of the information seen online is a result of some form of targeting. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts</li> <li>• How the targeting is done</li> <li>• The concept of clickbait and how companies can use it to draw people to their sites and services</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSHE</li> <li>• <b>or</b> RSE</li> <li>• Health education</li> <li>• Computing</li> </ul>
<b>How to stay safe online</b>		
Online abuse	<p>Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• The types of online abuse, including sexual harassment, bullying, trolling and intimidation</li> <li>• When online abuse can become illegal</li> <li>• How to respond to online abuse and how to access support</li> <li>• How to respond when the abuse is anonymous</li> <li>• The potential implications of online abuse</li> <li>• What acceptable and unacceptable online behaviours look like</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSHE</li> <li>• <b>or</b> RSE</li> <li>• Computing</li> <li>• Citizenship</li> </ul>
Challenges	<p>Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal</li> <li>• How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why</li> <li>• That it is okay to say no and to not take part in a challenge</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSHE</li> <li>• RSE</li> <li>• PSD</li> </ul>

	<ul style="list-style-type: none"> <li>• How and where to go for help</li> <li>• The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges</li> </ul>	
Content which incites violence	<p>Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• That online content (sometimes gang related) can glamorise the possession of weapons and drugs</li> <li>• That to intentionally encourage or assist in an offence is also a criminal offence</li> <li>• How and where to get help if they are worried about involvement in violence</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• <b>PSHE</b></li> <li>• RSE</li> </ul>
Fake profiles	<p>Not everyone online is who they say they are. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• That, in some cases, profiles may be people posing as someone they are not or may be 'bots'</li> <li>• How to look out for fake profiles</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSHE</li> <li>• RSE</li> <li>• Computing</li> </ul>
Grooming	<p>Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• Boundaries in friendships with peers, in families, and with others</li> <li>• Key indicators of grooming behaviour</li> <li>• The importance of disengaging from contact with suspected grooming and telling a trusted adult</li> <li>• How and where to report grooming both in school and to the police</li> </ul> <p>At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.</p>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• <b>PSHE</b></li> <li>• RSE</li> </ul>
Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience)	This risk or harm is covered in the

	<p>can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content</li> <li>• The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely</li> <li>• That online behaviours should mirror offline behaviours and that this should be considered when making a livestream</li> <li>• That pupils should not feel pressured to do something online that they would not do offline</li> <li>• Why people sometimes do and say things online that they would never consider appropriate offline</li> <li>• The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next</li> <li>• The risks of grooming</li> </ul>	<p>following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSHE</li> <li>• PSD</li> </ul>
Pornography	<p>Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• That pornography is not an accurate portrayal of adult sexual relationships</li> <li>• That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour</li> <li>• That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSD</li> <li>• RSE</li> </ul>
Unsafe communication	<p>Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSHE</li> <li>• PSD</li> <li>• Computing</li> </ul>

	<ul style="list-style-type: none"> <li>● How to identify indicators of risk and unsafe communications</li> <li>● The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before</li> <li>● What online consent is and how to develop strategies to confidently say no to both friends and strangers online</li> </ul>	
<b>Wellbeing</b>		
Impact on confidence (including body confidence)	<p>Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● The issue of using image filters and digital enhancement</li> <li>● The role of social media influencers, including that they are paid to influence the behaviour of their followers</li> <li>● The issue of photo manipulation, including why people do it and how to look out for it</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● PSHE</li> <li>● PSD</li> </ul>
Impact on quality of life, physical and mental health and relationships	<p>Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time)</li> <li>● How to consider quality vs. quantity of online activity</li> <li>● The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear of missing out</li> <li>● That time spent online gives users less time to do other activities, which can lead some users to become physically inactive</li> <li>● The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● PSHE /PSD</li> </ul>



	<ul style="list-style-type: none"> <li>● That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support</li> <li>● Where to get help</li> </ul>	
Online vs. offline behaviours	<p>People can often behave differently online to how they would act face to face. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives</li> <li>● How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● PSHE</li> <li>● RSE</li> </ul>
Reputational damage	<p>What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>● Strategies for positive use</li> <li>● How to build a professional online profile</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>● PSHE</li> <li>● RSE</li> </ul>
Suicide, self-harm and eating disorders	<p>Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.</p>	