ROSEMEAD PREPARATORY SCHOOL & NURSERY
DULWICH



IT Policy

Policy Owner: Deputy Head (Pastoral)

ISSR Reference: N/A

Reviewed: Michaelmas 2025

Approved: Full Governing Body Michaelmas 2025

Next Review: Michaelmas 2026

Version Control Information

Reason for Amendment	Role	Date	Main Changes
Creation of new policy	Chief Operating Officer	Michaelmas 2024	New policy
Interim review	Chief Operating Officer	Trinity 2025	Review of roles and responsibilities
Annual review	Deputy Head Pastoral	Michaelmas 2025	

Contents

1. Aims and introduction 4
2. Legislation 4
3. Roles and responsibilities 5
4. Educating pupils about online safety 8
5. Educating parent / carers about online safety 8
6. Cyber-bullying 9
7. Acceptable use of the internet in school and outside of school whilst using school devices 11
8. Pupils using mobile devices in school 12
9. How the school will respond to issues of misuse by pupils 12
10. Training 13
11. Monitoring arrangements 14
12. Links with other policies 14
Appendix A: EYFS and Pre-Prep acceptable use agreement 15
Appendix B: Prep acceptable use agreement 14

1. Aims and introduction

1.1 Policy aims

This policy is applicable to pupils and parents / carers of Rosemead Preparatory School & Nursery. Rosemead Preparatory School & Nursery (the 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 at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers the school to protect and educate the whole school community in its use of technology, including mobile and smart technology, which in this policy is referred to as 'mobile phones'
- Establish clear mechanisms to identify, intervene and escalate an incident where appropriate.

1.2 Approach to online safety: risk categories

The school's 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.

2. Legislation

This policy is based on advice from the Department for Education (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education and informed by the following guidance:

- Teaching online safety in schools
- Preventing and tackling bullying and cyberbullying: advice for teachers and school staff
- Relationships and sex education
- Searching, screening and confiscation.

It also refers to the DFE's guidance on protection of children from radicalisation and reflects legislation, including but not limited to the Education Act 1996 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is 'a good reason' to do so.

3. Roles and responsibilities

3.1 St Dunstan's Education Group

The governing body has ultimate responsibility for monitoring this policy but will delegate day-to-day responsibility to the Chief Executive Officer (CEO) of St Dunstan's Education Group and the Head of Rosemead Preparatory School & Nursery. The governing body has a duty to ensure that:

- All staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring
- The Safeguarding Link Governor attends annual meetings with the Designated Safeguarding Lead (DSL) to discuss online safety, requirements for training and to review online safety logs provided by the Director of Digital Services
- All pupils are taught how to keep themselves and others safe, including keeping themselves safe online
- That the school has appropriate filtering and monitoring systems in place on school devices and school networks, and to annually review their effectiveness. This includes assessing the following requirements:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
    - Reviewing and monitoring provisions at least annually
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning

- Having effective monitoring strategies in place that meet the school's safeguarding needs.

The governor who oversees online safety is the Safeguarding Link Governor.

3.2 The Head of Rosemead Preparatory School & Nursery

The Head of Rosemead Preparatory School & Nursery (Head of the school) is responsible for ensuring that staff understand this policy, and that it is being implemented consistently across the school.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in the Child Protection and Safeguarding Policy. The DSL takes the lead responsibility for online safety in the school, including:

- Supporting the Head of Rosemead Preparatory School & Nursery in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head of the school and governing body to review this policy annually and to ensure that the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring and systems and processes that are in place
- Working with the Head of School Digital Services and the Director of Digital Services to ensure that appropriate systems and processes are in place and to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's Safeguarding and Child Protection Policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's Expected Pupil Behaviour policy
- Updating and delivering staff training on online safety at least annually
- Liaising with other agencies and / or external services if necessary.

3.4 The Director of Digital Services

The Director of Digital Services, supported by the Head of School Digital Services, is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Testing the school's filtering and monitoring systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that online safety incidents are logged and dealt with appropriately in accordance with this policy.

3.5 Staff

All staff, including contractors and agency staff, and volunteers, as appropriate, are responsible for:

- Maintaining an understanding of this policy
- Agreeing to the staff terms on acceptable use of the school's IT network and internet as detailed in the Electronic Information and Communication Systems Policy and ensuring that pupils follow the school's pupil terms on acceptable use (Appendix A).
- Knowing that the DSL is responsible for the filtering and monitoring of systems and processes, and being aware of how to report to incidents of those system or processes failing by raising an alert on CPOMS, or alerting the Digital Services team
- Following the correct procedures, by contacting the Digital Services team, if they need to bypass the filtering and monitoring system for education or work purposes
- Working with the DSL to ensure that online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are deal with appropriately in line with the school's Expected Pupil Behaviour Policy
- Responding appropriately to reports and concerns about sexual violence and / or harassment, both online and offline, and maintaining an attitude of 'it could happen here.'

3.6 Pupils, parents and carers

Pupils, parents and carers are expected to:

- Read, understand and agree to the terms on acceptable use of the school's IT systems and networks (Appendix A)

- Engage with any e-safety training and advice provided.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum, the learning outcomes at each stage will be:

Pre-Prep	Use technology safely, keeping personal information private Use technology safely and respectfully, keeping personal information private Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
Prep	Use technology safely, respectfully and responsibly Recognise acceptable and unacceptable behaviour Identify a range of ways to report concerns about content and contact
End of Year 6	Understand that sometimes people behave differently online, including by pretending to be someone they are not Understand that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when individuals are anonymous Understand the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them Understand how to critically consider their online friendships and sources of information, including awareness of the risk associated with people they have never met Understand what information and data is shared and used online Understand what sorts of boundaries are appropriate in friendships with peers and others, within a digital context Understand how to respond safely and appropriately to adults they may encounter online

5. Educating parent / carers about online safety

The school will raise parents / carers' awareness of internet safety in letters, or other communications home, and also offer at least one annual parent e-safety session. This information will include:

- What systems the school uses to filter and monitor online use
- What pupils are asked to do online, including the sites they will be asked to access.

Concerns or queries about this policy should be raised with the relevant form tutor in the first instance. Further advice may be sought from the DSL.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, the school will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. Pupils will be taught how they can report any incidents and will be encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

As part of wider safeguarding training, all staff, governors and relevant volunteers receive training on cyber-bullying, its impact and ways to support pupils (see Section 10).

The school also sends information on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Expected Pupil Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. The DSL will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

As detailed in the school's Expected Pupil Behaviour Policy, the CEO, the Head of the school, and any member of staff authorised to do so by these two role holders, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and / or;
- Is identified in the school Expected Pupil Behaviour Policy as a banned item for which a search can be carried out, and / or;
- Is evidence in relation to an offence.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member must reasonably suspect that the device has, or could be used to:

- Cause harm, and / or;
- Undermine the safe environment of the school or disrupt teaching, and / or;
- Commit an offence.

If inappropriate material is found on the device, the DSL will decide on a suitable response in accordance with the school's Expected Pupil Behaviour Policy. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that is continued existence is likely to cause harm to any person, and / or;
- The pupil, or the parent / carer refuses the delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they must:

- **NOT** view the image

- Confiscate the device and report the incident to the DSL immediately, who will decide on what to do next, in accordance with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's Expected Pupil Behaviour Policy.

Any complaints about searching for, or deleting, inappropriate images or files on pupils' electronic devices will be dealt with through the St Dunstan's Education Group's Complaints Policy and Procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The school recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. The school will treat any use of AI to bully pupils in line with the school's Expected Pupil Behaviour and Anti-Bullying policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of the internet in school and outside of school whilst using school devices

All pupils, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet. EYFS and Pre-Prep pupils do this annually in class with their form teacher signing on their behalf. Prep pupils complete this independently via an online form. Visitors are expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling

the duties of an individual's role.

The school will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate. The following systems are in place to enable the school to monitor and filter web content and emails.

Web Filter
Cloudflare DNS and Unifi Content Filtering
Monitoring software for pupil devices (on and off site)
Smoothwall Cloud Filter
Anti-Virus Software
Bit Defender GravityZone

These systems are provided by third-party companies who also ensure the usability, uptime and availability of these systems. Any person that logs onto a device and joins a school network will pick up the filtering and monitoring system for the school the device is being used at.

8. Pupils using mobile devices in school

Pupils in Nursery up to Year Five are not permitted to bring mobile devices, including phones, music players tablet computers, into school. Year Six pupils who travel to and from the school independently, may bring a mobile device to school once approval has been given by the parent / carer for independent travel. It must be switched off and handed into the office at the beginning of the school day.

9. How the school will respond to issues of misuse by pupils

Where a pupil misuses the IT systems or internet, the school will follow the procedures set out in the Expected Pupil Behaviour and this IT Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training annually as part of safeguarding training, as well as relevant updates as required (for example through emails, briefings and CPD sessions). Staff are expected to understand that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Physical abuse, sexual violence and initiation / hazing type violence can contain an online element
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and / or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and their deputies will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in the school's Child Protection and Safeguarding Policy.

11. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed by the Designated Safeguarding Lead, Director of Digital Services and Chief Operating Officer annually. At every review, the policy will be approved by the Education Committee.

12. Links with other policies

This IT Policy links to the following policies:

- Expected Pupil Behaviour (school)
- Information Security (Group)
- Safeguarding and Child Protection (school)

Appendix A: EYFS and Pre-Prep acceptable use agreement

I understand that I must use Rosemead Preparatory School & Nursery's systems responsibly to ensure there is no risk to anyone's safety. I agree to follow the rules below when using IT systems at the school and at home.

Device Care

- I will look after any device and accessories (keyboard/mouse/charger) that I use.
- I will not install software on any school device.
- I will keep my username and password safe.
- I will log in to IT systems using only my username and password. I will not share my username or password with anyone else or try to use anyone else's username or password.
- I will only use IT at school when my teacher asks my to do so. I will not use school devices for accessing inappropriate sites.
- I will only open and delete my files and not other people's files.
- I will not click any documents or links without checking with a teacher.
- I will always log off or shut down my computer when I have finished.
- I understand that the school can check my computer and that my parents/carers can be contacted if staff are concerned about my e-safety.

Responsibility

- I understand that I am responsible for my behaviour and actions when using technology or the internet.
- The emails and instant messages I send will be polite and sensible.

Internet security and online content

- I will never give out my personal information online unless advised by my teacher.
- I will never arrange to meet anyone offline.
- I will never upload any images of school activities to any social networking site.
- I will not deliberately look for, save or send anything that could be upsetting.
- I understand that sending a message to deliberately make someone feel upset is unacceptable.
- If I see anything upsetting on the school devices, I will turn the screen off and tell an adult.
- I understand that the school checks what I do on the computers to prevent me from finding anything upsetting online.
- I will not copy work from the internet and claim it as my own.

- I understand that the sanctions for misuse of IT may include me not being allowed to use school devices.

Pupil Name: _____ Form: _____

Pupil Signed: _____ Date: _____

Appendix B: Prep Acceptable use agreement

I understand that I must use Rosemead Preparatory School & Nursery's (the school) systems responsibly to ensure there is no risk to my safety or the safety and security of the systems and other users. I agree to follow the rules below when using IT systems at the school and at home.

Device Care

- I will take care of the device (including its charger and case), only transporting devices while in a case.
- I will not install or attempt to install software on any school device.
- I will keep my username and password safe.
- I will log in to IT systems using only my username and password. I will not share my username or password with anyone else or try to use another pupil's or staff member's username and password.
- I will only use IT at school for educational purposes as directed by my teacher. I will not use school devices for accessing gaming sites, social networking sites, chat rooms, or visit any other sites I know, or suspect to be, inappropriate.
- I will only open and delete my files and not those of others.
- I will not open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- I will always log-off or shut down my computer when I have finished using it.
- I understand that the school can check my computer or other devices and that my parents/carers can be contacted if staff are concerned about my e-safety.

Own devices

- If I am in Year Six and authorised to bring a mobile phone, or other personal electronic device to school, I will hand it in to the office at the beginning of the school day and will not use it without a teacher's permission.
- I understand that if my device is damaged intentionally or because of a lack of care, the school will charge my parents/carers the insurance claim excess cost.

Responsibility

- I understand that I am responsible for my behaviour and actions when using technology or the internet.

- The emails and instant messages I send will be polite and sensible, whether to fellow pupils or teachers.

Internet Security and Online Content

- I will never give out my personal information, or that of other people, online unless it is on a trusted website, as advised by my teacher.
- I will never arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.
- I will never upload any images of school activities to any social networking site.
- I will not deliberately look for, save or send anything that could be perceived as upsetting, threatening or offensive.
- I understand that sending a message with the deliberate intention of making another person feel offended, embarrassed, threatened, or hurt is **bullying** and will be dealt with according to the school Anti-Bullying Policy.
- If I see anything upsetting or inappropriate on the school devices, I will immediately turn the screen off and tell a member of staff, my parents/carers, or another appropriate adult.
- I understand that the school uses filtering and monitoring software to prevent me from: a) accessing inappropriate content (filtering), and b) creating or searching for inappropriate content (monitoring). This monitoring software will be used on school devices both in and out of school.
- I will not copy and plagiarise content from the internet, nor infringe copyright. I will not claim the work of others as my own.
- I understand that the sanctions for misuse of IT will align with the school's Behaviour Policy and may include suspension of IT privileges or more serious sanctions.

Pupil Name: _____ Form: _____

Pupil Signed: _____ Date: _____