RADLETT
PREPARATORY SCHOOL

ONLINE SAFETY POLICY

INCLUDING ONLINE SAFETY
ACCEPTABLE USE AGREEMENTS

Approved by:	Mrs L Flynn	**Signature:**	
Written by:	Mr T King		
Last reviewed on:	October 2023		
Next review due by:	October 2024		

Table of Contents

1. Introduction

Radlett Preparatory School recognises that the internet, mobile and digital technologies provide a good opportunity for children and young people to learn, socialise and play, provided they are safe. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that **all** pupils and staff will be able to use the internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in the safeguarding of children. Below are the four main areas of risk, as identified in Keeping Children Safe in Education (September 2023). The NSPCC define the four main areas as:

Content

Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

Commerce

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

2. Roles and Responsibilities

Directors

The board of Directors has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The board of Directors will make sure 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 board of Directors will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The board of Directors will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The board of Directors should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The board of Directors must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering 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 their safeguarding needs.

All Directors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school’s ICT systems and the internet (see appendices)
- Ensure that online safety is a running and interrelated theme while devising and implementing a whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a ‘one size fits all’ approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school’s designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal and board of Directors to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the school's IT consultant to make sure the appropriate systems and processes are in place
- Working with the Principal, the IT consultant, Computing and Digital Learning lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (Appendix H) 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 behaviour policy
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or board of Directors
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The School IT Consultant & Computing and Digital Learning Lead

The school IT consultant & Computing and Digital Learning Lead are 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
- Conducting a full security check and monitoring the school's IT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (Appendix H) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendices B & Bi), and ensuring that pupils follow the school's terms on acceptable use (appendices Ci &Cii)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by liaising with both the school's IT consultant and the Computing & Digital Learning Lead.
- Following the correct procedures by discussing these with the school's IT consultant if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (appendix H) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices Ci & Cii)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

3. Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school directors
- peripatetic teachers/coaches, supply teachers, student teachers
- other adults working on school premises – (office, medical, maintenance etc.)
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities.

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, through the school website, social media, via parent mail, in newsletters, via our accredited National Online Safety website and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, GDPR, health and safety, social media, behaviour, anti-bullying and PSHCE policies.

4. Policy and procedure

The school seeks to ensure that the internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use the internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and all other visitors to the school.

Use of email

All Staff use a school email account for all official communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils may only use school approved accounts on the school system and only for educational purposes. Where required parent/carer permission will be obtained for the account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff and pupils should not open emails or attachments from suspect sources and should report their receipt to the network manager or online safety co-ordinator.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with pupils/ families.

- When working with pupils searching for images should be done through Google Safe Search, Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)

- Adult material that breaches the Obscene Publications Act in the UK

- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status

- Promoting hatred against any individual or group from the protected characteristics above

- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy

- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect.

Users must not

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school
- Upload/download content onto/into our virtual learning environment without prior permission
- Must not use our virtual learning environment for social 'chatting' purposes. Our virtual learning environment is to be used to ask questions that are related to the work set by teachers ONLY.

Only a school device may be used to conduct school business outside of school.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the Principal.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See GDPR policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to staff. Staff and pupils may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is in the personnel file.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers should not use personal mobile phones and devices on school premises unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child. When a parent/carer is on school premises, their phone/s must be switched off and out of sight. Please refer to our Child Protection and Keeping Children Safe in Education polices for further information.

Pupils are NOT allowed to bring personal mobile phones, or any internet enabled device such as watches/tablets, etc. to school.

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

We encourage our staff not to use personal mobiles to access school emails and data. All staff have been told that they should only access emails if their mobile phones are password protected.

New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with the online safety co-ordinator and or the Principal before they are brought into school.

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL, the Principal or online safety co-ordinator. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

5. Curriculum

Online safety is embedded within our curriculum. The school provides a comprehensive curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use the internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work also includes:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity

- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment

- Developing critical thinking skills in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)

- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others

- Understanding the permanency of all online postings and conversations

- Understanding relevant legislation, including copyright, and the importance of respecting other people’s information, reputation and images

- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help

6. Staff Training

Staff are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of the internet, mobile and digital technologies.

New staff are provided with a copy of the online safety policy and must sign the school’s Acceptable Use Agreement as part of their induction and before having contact with pupils.

Any organisation working with children based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (Appendix B).

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (Appendix B).

7. Working in Partnership with Parents/Carers

The school works closely with families to help ensure that children can use the internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website and by other means.

Parents/carers are asked to read, discuss and co-sign with each child the Acceptable Use Agreement. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities. The support of parents/carers is essential to implement the online safety policy effectively and keep all children safe.

8. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly to ensure they are effective and that the risks to pupils and staff are minimised.

All breaches of this policy must be reported and all reported incidents are logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. All incidents need to be reported to the online safety co-ordinator.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of the internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

The Principal and Directors receive half termly summary data on recorded online safety incidents for monitoring purposes. In addition, the Principal and Directors ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

9. Appendices of the Online Safety Policy

A. Online Safety Acceptable Use Agreement - Staff

B. Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers, visitors, volunteers and parent/carer helpers working in the school (working directly with children or otherwise)

Bi. Online Safety Acceptable Use Agreement – Ad hoc visitors

Ci Online Safety Acceptable Use Agreement Primary Pupils (Infants – Reception, Year 1 and Year 2)

Cii Online Safety Acceptable Use Agreement Primary Pupils (Year 3 to Year 6 Pupils)

D. Online safety policy guide - Summary of key parent/carer responsibilities

E. Guidance on the process for responding to cyberbullying incidents

F. Guidance for staff on preventing and responding to negative comments on social media

G. Online safety incident reporting form

H. Online safety incident record

I. Online safety incident log

Appendix A - Online Safety Acceptable Use Agreement – Staff

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff are aware of their responsibilities in relation to their use. All staff are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Principal. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply, and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety co-ordinator and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptional use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the computing and online safety co-ordinator.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager and/or the principal.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become ‘friends’ with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or ridicule the school, its staff, directors, parents/carers or pupils. Privileged information must remain confidential.

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.
I will not upload any material which is about, or which references the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member. For visitors that need access to the school network, a temporary password will be set-up for their use.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include

- Photographs must be kept securely and used appropriately, whether in school or taken off the school premises
- Personal data can only be taken out of school or accessed remotely when authorised by the Principal
- Personal or sensitive data taken off site must be encrypted.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email address/es for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices (including wearable) in school is at the discretion of the Principal.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices unless a closed, monitored system has been set up by the school.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the network manager or/and online safety co-ordinator.

Promoting online safety

I understand that online safety is the responsibility of all staff and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.
I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, visitors, pupils or parents/carers) to the DSL.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom or elsewhere in the school; this will include the acceptability of other material visible, however briefly, on the site. I will not free surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance from the Principal for the material I plan to use.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as director.

Signature ……..……………………………… Date ……………………

Full Name …………………………….. (printed)

Job title ……………………………………………………………………

Appendix B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers, visitors, volunteers and parent/carer helpers
(Working directly with children or otherwise)

Radlett Preparatory School

Online safety co-ordinator

Designated Safeguarding Lead (DSL)

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all adults are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the online safety co-ordinator. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety co-ordinator and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptional use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the online safety co-ordinator.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager and/or the Principal.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the Principal.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over 13 and parents/carers through the school's organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or ridicule the school, its staff, directors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material which is about or which references the school or its community on my personal social networks without obtaining written permission from the principal.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone else. For visitors that need access to the school network, a temporary password will be set-up for their use.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.

- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on an adult's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the principal.

Use of Email

I will use my professional or formal student email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices (including wearables) in school is at the discretion of the principal.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the network manager and/or the online safety co-ordinator.

Promoting online safety

I understand that online safety is part of my responsibility, and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSL.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom or elsewhere in the school; this will include the acceptability of other material visible, however briefly, on the site. I will not free surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance from the Principal for the material I plan to use.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ……..……………………………….…   Date ……………………

Full Name ……………………………………………………………………………. (Please use block capitals)

Job Title/Role ………………………………….……………………..…………

Appendix Bi - Online Safety Acceptable Use Agreement – Ad hoc visitors, volunteers and parent/carer helpers

(Working directly with children or otherwise)

Radlett Preparatory School

Online safety co-ordinator

Designated Safeguarding Lead (DSL)

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all adults and visitors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the online safety co-ordinator. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access
I will not access or attempt to access any sites that contain any discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive.

Online conduct
I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

Social networking
I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Passwords
I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone else. For visitors that need access to the school network, a temporary password will be set-up for their use.

Data protection
I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device or have a prior agreement with the school.

- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos
I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the Principal.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning.

Promoting online safety

I understand that online safety is part of my responsibility, and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way, to the DSL.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom or elsewhere in the school; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ………………………………………… Date ……………………

Full Name ……………………………………………………………………………… (Please use block capitals)

Job Title/Role …………………………………………………………………

Appendix Ci - Online Safety Acceptable Use Agreement Primary Pupils

(Infants – Reception, Year 1 and Year 2)

My Online Safety Rules

- I will only use school computing equipment for activities when given permission by an adult.
- In school, I will only open or delete my files when told by an adult.
- I will make sure that everything I make or type on a computer is responsible, polite and sensible. I will always be kind and respectful.
- If I see or hear anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe on a computer, screen or tablet, I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including name, phone number, home address, interests, schools name or club names. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- I will not upload, post or send any images, photographs, videos or live streams without permission from an adult.
- I will not upload any images, videos, sounds or words that **could** upset someone else.
- I understand that everything I do or receive online can be seen, now and in the future. I know it is important to build a good online reputation.
- I understand that personal devices are NOT allowed in school, I will follow this rule. I will not assume that new devices can be brought into school without getting permission.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will investigate it and may need to take action.
- I understand that I will not upload/download content onto our virtual learning environment without prior permission.
- I understand that I must not use our virtual learning environment for social 'chatting' purposes. Our virtual learning environment is to be used to ask questions that are related to the work set by my teachers ONLY.

Appendix Cii - Online Safety Acceptable Use Agreement Primary Pupils

(Year 3 to Year 6 Pupils)

My Online Safety Rules

- I will only use school computing equipment for activities when given permission by an adult.
- I will not use my personal email address or other personal accounts in school when doing schoolwork.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only use email (in the computing suite) when learning about online communication and when given permission by an adult.
- In school, I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I see or hear anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, on a computer, screen or tablet, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including name, phone number, home address, interests, schools name or club names. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- I will not upload, post or send any images, photographs, videos or live streams without permission from an adult.
- I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are, and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that personal devices are NOT allowed in school, I will follow this rule. I will not assume that new devices can be brought into school without getting permission.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will investigate it and may need to take action.
- I understand that I will not upload/download content onto our virtual learning environment without prior permission.
- I understand that I must not use our virtual learning environment for social 'chatting' purposes. Our virtual learning environment is to be used to ask questions that are related to the work set by my teachers ONLY.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life.

We want all children to be safe and responsible when using any device. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with the online safety co-ordinator.

Please return the signed sections of this form which will be kept on record at the school.

Pupil agreement

Pupil name……………………………………

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature…………………………………………………………………..

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)………………………………………………

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

Date ……………………

Appendix D - Online Safety Acceptable Use Agreement for Parents and Carers

Online channels are an important way for parents/carers to communicate with, or about, our school.
The school uses the following channels:

- The school website - http://www.radlettprep.co.uk
- Email/text/parent mail groups for parents (for school announcements and information)
- Our virtual learning platform
- School Facebook page

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- be respectful towards members of staff, and the school, at all times;
- be respectful of other parents/carers and children;
- direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure.

I will not:

- use private groups, or personal social media to complain about or criticise members of staff. This is not constructive, and the school can't improve or address issues if they aren't raised in an appropriate way;
- use private groups, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident;
- upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers;
- take/capture any photos/videos and/or recordings of our live teaching lessons on our virtual learning platform;
- use personal mobile phones and devices on school premises unless otherwise informed, e.g. for specific events and activities.

I understand that when on school premises, <u>all mobile devices</u> must be switched off and out of sight.

<u>Parent(s)/Carer(s) agreement</u>

Parent(s)/Carer(s) name(s)…………………………………………………….

Parent/carer signature……………………………………..

Name of child: …………………………………………….

Date …………………………………………………………

Appendix E - Online safety policy guide - Summary of key parent/carer responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.
- Parents/carers should not use personal mobile phones and devices on school premises unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child. When a parent/carer is on school premises, their phone/s must be switched off and out of sight. Please refer to our Child Protection and Keeping Children Safe in Education polices for further information.

- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.

- Any parent/carer distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Appendix F - Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.

- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, Principal) and staff members should seek support from their line manager or a senior member of staff (SLT).

- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the Principal so that the circumstances can be recorded.

- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.

- A senior member of staff will conduct an investigation.

- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix G - Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix E (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

  As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

  If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the Principal will need to follow the school's safeguarding procedures.

  If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

  Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

- Addressing negative comments and complaints

  Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings.
- Ask for the offending remarks to be removed.
- Explore the complainant’s grievance.
- Agree next steps.
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;

- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Appendix H - Online safety incident reporting form

Any member of the school community can raise a concern about an online safety incident. If you have witnessed or experienced an incident please complete the form below to help us to address the issue. It is important that you provide as much detail as possible. Once completed please hand this report to the online safety co-ordinator.

Name of person reporting incident:				
Signature:				
Date you are completing this form:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				
Time of incident(s):				

Who was involved in the incident(s)?	Full names and/or contact details
Children/young people	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyber bullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of acceptable use agreement, please specify			

Full description of the incident	What, when, where, how?

Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence available but do not attach.

Thank you for completing and submitting this form.

Appendix I - Online safety incident record

Name of person reporting incident:				
Date of report:				
Where did the incident take place:	Inside school?		Outside school?	
Date of incident(s):				

Time of incident(s):	

Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age inappropriate websites, apps and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement			
Other, please specify			

Full description of the incident	What, when, where, how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc

Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to online safety Coordinator/DSL/ DSP/Principal	
Safeguarding advice sought, please specify	
Referral made to HCC Safeguarding	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Brief summary of incident, investigation and outcome (for monitoring purposes)	

Appendix J - Online safety incident log

Summary details of ALL online safety incidents will be recorded on this form by the online safety coordinator or other designated member of staff. This incident log will be monitored half termly and information reported to SLT and directors.

Date & time	Name of pupil or staff member Indicate target (T) or offender (O)	Nature of incident(s)	Details of incident (including evidence)	Outcome including action taken
