Roundwood Primary School

Name of Policy	**Online Safety Policy**
Date of last review	January 2021
Date of next review	January 2022*
Governing Body Committee Responsible	Resources
Member of Staff responsible	Headteacher

*Unless there is significant change in legislation

Table of Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of **all pupils, staff and governors** within the school community at Roundwood Primary with respect to the safe use of internet, mobile and digital technologies.
- Safeguard and protect the children and staff of Roundwood Primary School.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of internet, mobile and digital technologies for educational, personal, or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies and national legislation.
- Ensure that **all pupils, staff and governors** within the school are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse, sex exploitation and criminal exploitation
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites, incitement to extremism and radicalisation
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords
- Sexual exploitation and criminal exploitation

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film) (Ref Ofsted inspection guidance Jan 2014)

2. Scope

This policy applies to all members of Roundwood Primary School community (including staff, pupils, school governors, volunteers, parents, carers, visitors and community users) who have access to and are users of school computer systems, both in and out of Roundwood Primary School.

The school provides online safety information for parents and carers, for example, through the website, in newsletters, in specialised online safety newsletters and by providing parental access to National Safety Online where parents can complete their own online safety training.

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, Keeping Children Safe in Education 2020, GDPR, Health and Safety, Remote Learning, Behaviour, Anti-Bullying and RSE policies.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy (under Policies & Downloads on our website).

The school will deal with such incidents within this policy and associated Behaviour Policy and Anti-Bullying policy (under Policies & Downloads on our website) and will, where known, inform parents or carers of incidents of inappropriate online safety behaviour that take place out of school.

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and stored on the shared network drive.
- Policy to be part of school induction pack for new staff.
- Acceptable Use Agreements discussed with pupils at the start of each year and revisited termly.
- Acceptable Use Agreements to be issued to whole school community, usually on entry to the school.
- Parental Acceptable Use Agreements to be held in pupil files.
- Policy will be accepted by staff and pupils through the network on a termly basis.

3. Responsibilities

The head teacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named Online Safety Lead in this school is Kate Hooft.
All breaches of this policy must be reported to Kate Hooft.
All breaches of this policy that may have put a child at risk must **also** be reported to a DSL, Heather Brennan, Lisa Kraushaar or Hannah Smith.

Organisations that are renting space from the school, for example Jousters, and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements.

However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount, and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

Role	Key Responsibilities
Headteacher / Designated Child Protection Lead	• To take overall responsibility for online safety provision
	• To take overall responsibility for data and data security (SIRO)
	• To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements
	• To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant
	• To be aware of procedures to be followed in the event of a serious online safety incident.
	• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. Network Manager)
	• To ensure that an online safety incident log is kept up to date
	• To liaise with the Local Authority and relevant agencies when necessary • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contacts with adults/strangers • potential or actual incidents of grooming • cyber-bullying and use of social media • Oversees the delivery of the online safety • element of the Computing curriculum
Computing Subject Leader	• Oversees the delivery of the online safety element of the Computing curriculum • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contacts with adults/strangers • potential or actual incidents of grooming • cyber-bullying and use of social media
Governors – including the Governor responsible for Safeguarding	• Ensures that the school follows all current online safety advice to keep the children and staff safe
	• Approves the Online Safety Policy and reviews the effectiveness of the policy
	• Supports the school in encouraging parents and the wider community to become engaged in online safety activities
Network Manag	• Reports any online safety related issues that arises, to the SLT, DSLs and Computing Subject Leader

	• Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are changed termly
	• Ensures that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date
	• Ensures the security of the school computing system
	• Ensures that access controls / encryption exist to protect personal and sensitive information held on the school network in lines with the school's encryption guidelines
	• Applies and regularly updates the school's policy on web filtering
	• Informs the LA/ web filtering provider of issues relating to the filtering applied
	• Monitors the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
	• Regularly monitors the use of the network, data systems and email in order that any misuse or attempted misuse can be reported to the Online Safety Lead /Head teacher for investigation, action, or sanction
	• Ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
	• Maintains up-to-date documentation of the school's e-security and technical procedures • Ensures that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• Embed online safety issues in all aspects of the curriculum and other school activities in line with the Computing scheme of work
	• Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), using any issues that arise as teaching opportunities
	• Ensure that pupils are made aware of research skills and are aware of legal issues relating to electronic content such as copyright laws and creative commons licences.
All staff	• Read, understand, and help promote the school's online safety policies and guidance
	• Read, understand, accept, and adhere to the Staff Acceptable Use Agreement
	• Demonstrate an awareness of online safety issues related to the use of mobile phones, cameras and handheld devices, monitoring their use and implementing current school policies with regard to these devices
	• Report any suspected misuse or problem to the Head teacher • Record any online safety issues on the online safety incident reporting form and discuss it with the Head teacher
	• Maintain an awareness of current online safety issues and guidance e.g. through CPD
	• Model safe, responsible, and professional behaviours in their own use of technology
	• Ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

	• Are responsible for reading the school's online safety policy and using the school computing systems, accordingly, including the use of mobile phones, and handheld devices.
Pupils	• Read, understand, accept and adhere to the Pupil Acceptable Use Policy
	• Have an age appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
	• Understand the importance of reporting abuse, misuse, or access to inappropriate materials
	• Know what action to take if they or someone they know feels worried or vulnerable when using online technology • Know and understand school rules on the taking / use of images and on cyber-bullying • Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school • Understand their responsibility including the benefits and risks of using the Internet and other technologies safely both in school and at home • Assist the school in the creation/ review of the computing curriculum through involvement in Pupil Voice activities • should have a good understanding of research skills and how to act responsibly and safely online • Year 6 pupils - Know and understand school policy on the use of mobile phones
Parents/carers	• Support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
	• Read, understand and promote the school's Pupil Acceptable Use Agreement with their children
	• Access the school website in accordance with the relevant school Acceptable Use Agreement
	• Consult with the school if they have any concerns about their children's use of technology • Should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety Acceptable Use Agreement form at time of their child's entry to the school • Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

All Users	• Are responsible for using the school computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to accept before being given access to school systems • Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences • Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so • Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school • Will be expected to know and understand school policies on the use of mobile phones. They should also know and understand school policies on the taking and using images and on cyber-bullying

4. Policy and procedure

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

The school expects everyone to use 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 governors and all other visitors to the school.

5. Use of email

Staff and governors should use a school email account or Governor Hub (Microsoft Teams) for all official school 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 should use school approved accounts on the school system for educational purposes. 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, governors, and pupils should not open emails or attachments from suspect sources and should report their receipt to their teacher or Kim James.

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

6. 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 Network Manager / Data Protection Officer (Kim James, Anna Hancock and Russel Farnhill) with details of the site/service and seek approval from a senior

leader. The terms and conditions of the service should be read and adhered to. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating online content.

- When working with pupils, searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or Kiddle/Swiggle 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: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation

- 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

As school does not provide staff with their own equipment, staff are encouraged to work from their own devices. When working remotely, staff are encouraged to use secure cloud based systems and are provided with an encrypted memory stick to save work on if necessary. If documents cannot be accessed and edited on secure cloud based systems and staff need to download documents from RMPortico and remote learning platforms they may have to save documents directly onto their desktop. If this is the case, they are asked to save the document to their memory stick straight away. Staff are asked to delete downloaded documents from their computer and empty their recycling bin at least weekly. Any documents containing names and personal data must be encrypted when saved (See document encryption list). Staff are reminded not to access photographs of children from home. The only exception to this is during periods of remote learning where parents may choose to email photographs of their children alongside their work. Staff are asked to delete these documents regularly.

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 Kate Hooft.

7. 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 approved staff as determined by Kate Hooft. 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 children.

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 located in the personnel file.

8. 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. The school does not encourage a member of staff to contact a pupil or parent/carer using their personal device unless it is essential e.g. during a period of remote learning, during a school trip.

- Parents/carers may only use personal mobile phones and devices in designated areas 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 unless there is a pre-specified permission from Kate Hooft. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Pupils in Year 6 are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. In lesson times all such devices must be switched off. Under no circumstance should pupils use their personal mobile devices/phones whilst on the school site.
- The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Personal mobiles may be used to access school email accounts but must never be used to access school data.

9. 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 Kate Hooft 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 head teacher or the Network Manager. 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.

Handling complaints:

The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- informing parents or carers.
- removal of Internet or computer access for a period
- referral to LA / Police.
- The Headteacher acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

10. Education and Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate 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 RSE curriculum, are central in supporting the delivery of online safety education.

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 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 will also include areas such as:

- 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 and the confidence to challenge and question what they see and read 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 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

- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help

- How the law can help protect against online risks and abuse

11. Video-Conferencing / Live Streaming Guidance for Staff and Pupils

Roundwood Primary School has a Remote Learning Policy which outlines our approach for pupils that will not be attending school, either as a result of government guidance, a bubble closure or in the event of a full

closure. During times of remote learning, we are aware that Online Safety and Safeguarding will continue to be paramount. As such staff and pupils must follow the guidance below:

Location

If a member of staff is leading or a learner is joining a video-conferencing call or live-streaming call from home or remotely they should:

- choose a neutral location that is appropriate and safe, e.g. a living room, a study or a kitchen
- reduce the possibility of the lesson being interrupted by other household members or pets.

Camera settings

- Carefully consider what is in view of the camera, i.e. check that the background is professional and does not contain images or information that should not be shared or that could be deemed inappropriate.
- It may be helpful to ask a 'critical friend' to check what is in view of the camera.
- Where possible, it is recommended that staff and learners change their background as standard practice.

Audio

The use of a headset with microphone (like those available with many mobile phones) is recommended for audio clarity.

Professional conduct

Staff should continue to work in the same professional manner as they would in the classroom and should undertake the following:

- Adhere to professional standards of dress when in front of the camera.
- Be conscious that in an online environment remarks are being heard by a number of learners and could be easily misconstrued.
- End the session for all participants, ensuring learners are not left alone and unsupervised in a lesson/session the practitioner has left.
- Be mindful of the need for confidentiality; especially if live-streaming a lesson from a venue where other adults or children are present.
- Staff should join the lesson/session before the scheduled time to ensure a proper connection and review the lesson plan so they feel prepared for an effective lesson/session.

Recording video-conferencing and live-streaming lessons and sessions

Video conferencing and live-streaming lessons and sessions are not recorded when children are in attendance.

Learner behaviour and etiquette

Setting out acceptable behaviours and expectations from the outset is essential for ensuring an effective and orderly lesson or session.

Staff should undertake the following.

- Make parents/carers aware of the expected behaviours and requirements including location to join the lesson/session and appropriate dress.
- Clearly communicate that 'classroom standard' of behaviour is expected from all participants.

- Create and agree clear ground rules to reflect the standard of behaviour expected based on their existing school or setting behaviour management policy.
- Explain the rules at the introduction of the lesson/session, e.g. who can speak, how to ask a question or ask for help.
- Consider using the chat, mute/unmute and the hand up/raised hands functions to make the most of the lesson or session.
- If this is the first time that lessons/sessions are delivered online, it may take some time to become familiar with the new environment. Using the chat function will allow the structured engagement with attendees.
- Continue to remind learners about agreed rules at the start of each lesson/session and outline how they can raise concerns if required.

External organisations

There may be occasions where schools or settings wish to video-conference or live-stream with external organisations. For instance to deliver a music lesson with a musician/group of musicians.
These lessons/sessions should be dealt with using the same safeguarding protocols as any other video-conferencing or live-streaming lesson or session as set out in this guidance, and with the additional points also recommended.

- The practitioner should set up and control the session, inviting the external organisation as a guest participant.
- The practitioner should clearly establish expectations and communicate the expectations set out in this guidance to the external provider.
- The practitioner should ensure they end the lesson/session for all when the lesson/session is over.
- Other professionals involved in providing online sessions with learners and/or their families will have been provided with clear guidance from their professional associations and/or employers and should follow these in conjunction with this guidance.

Staff and governor training

This school:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection in line with the school's policies on GDPR;
- Makes regular training available to staff on online safety issues and the school's online safety education program.
- Provides, as part of the induction process, all new staff 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.

Parent awareness and training

This school runs a rolling programme of advice, guidance, and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of safe online behaviour are made clear
- Information in school newsletters, additional online safety newsletters and on the school website.
- Suggestions for safe Internet use at home.
- Online Parental training through National Safety Online.

12. Records, monitoring and review

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order 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 will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. Any incidents are recorded using the online safety incident recording sheet.

The school supports pupils and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of 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.

Governors receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, governors 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.

Review and Monitoring

The online safety policy will be referenced from within other school policies: Child Protection Policy, Anti-Bullying Policy and Behaviour Policy.

- The school has a Network Manager (Kim James) and Safeguarding Governor (Amy Morle) who will be responsible for document ownership, review, and updates.

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

- The online safety policy has been written and reviewed by the Computing Subject Leader, the Network manager, the Head teacher and the Safeguarding Governor and is current and appropriate for its intended audience and purpose.

- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be discussed with all members of teaching staff.

Appendices of the Online Safety Policy

Appendix A - Online Safety Acceptable Use Agreement - Staff, Governors, Peripatetic teachers/coaches, trainee teachers, supply teachers

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 and governors are aware of their responsibilities in relation to their use. All staff, Peripatetic teachers/coaches, supply teachers, student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with Kate Hooft. 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 lead (Kate Hooft) 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. Exceptionally, 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 Kate Hooft and Kim James (Network Manager).

- 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, head teacher and others as required.

- 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 (unless they are paid staff members) 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 disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

- I will not upload any material about or references to 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.

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, taken off the school premises or accessed remotely

- Personal data can only be taken out of school or accessed remotely when authorised by the head teacher or governing body

- 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 or governor hub (Microsoft Teams) for all school business. 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 addresses or governor hub 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 in school is at the discretion of the head teacher.

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

- As school does not provide staff with their own equipment, staff are encouraged to work from their own devices. Staff are provided with an encrypted memory stick to save work on as necessary. When downloading documents from RMPortico, and remote learning platforms staff may have to save documents directly onto their desktop. If this is the case, they are asked to save the document to their memory stick straight away. Staff are asked to delete downloaded documents from their computer and

empty their recycling bin at least weekly. Any documents containing names and personal data must be encrypted when it is saved. Staff are reminded not to access photographs of children from home. The only exception to this is during periods of remote learning where parents may choose to email photographs of their children alongside their work. Staff are asked to delete these documents regularly.

Additional hardware/software

- I will not install any hardware or software on school equipment without permission of Kim James.

Promoting online safety

- I understand that online safety is the responsibility of all staff and governors, 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, governors, visitors, pupils or parents/carers) to the DSLs or Kate Hooft.

Classroom management of internet access

- I will pre-check for appropriateness all internet sites used in the classroom 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. I will also check the appropriacy of any suggested sites suggested for home learning.

- If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Kate Hooft, Heather Brennan or Hannah Smith.

Video conferencing

- I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and Designated Safeguarding Lead. A school-owned device should be used when running video-conferences, where possible.

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 a governor.

Signature ……..…….…… Date ……

Full Name ……..…….……..…… (printed)

Job title ……..…….……..……

Appendix B - Requirements for visitors, volunteers, and parent/carer helpers (Working directly with children or otherwise)

School name……..…...

Online safety lead ……..……

DSL ……..…..

This document is designed to ensure that you are aware of your responsibilities when using any form of electronic device in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the head teacher and/or DSL

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.

- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.

- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSL or head teacher is informed before I leave the school.

- I understand my visit to the school may give me access to privileged information about pupils, staff, school systems and plans. Such information should never be shared online, including on social media sites.

- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the head teacher.

- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content, I plan to use I will check with my contact in the school.

Appendix C - Online Safety Acceptable Use Agreement EYFS and Nursery Pupils

My online safety rules

- I will ask a grown-up before using computers and tablets.
- I will only use the computer / tablet to do activities I have been asked to do.
- I will be gentle with and look after the computers / tablets.
- I will ask a grown-up to help if I am stuck or if I think something has gone wrong.
- I know that if I follow the rules, I will be able to use the computers / tablets safely.

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 electronic 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 Lead, Kate Hooft.
Please complete the form below to show that you agree to follow this Agreement:

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……

Appendix D - Online Safety Acceptable Use Agreement KS1 Pupils

My online safety rules

- I always ask a teacher or suitable adult if I want to use the computers, tablets, or cameras.
- I only open activities and apps that an adult has told or allowed me to use.
- I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- I keep my passwords safe and will never use someone else's.
- I know personal information such as my address and birthday should never be shared online.
- I know I must never communicate with strangers online.
- I am always polite when I post online.

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 electronic 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 Lead, Kate Hooft.
Please complete the form below to show that you agree to follow this Agreement:

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……

Appendix E - Online Safety Acceptable Use Agreement KS2 Pupils

My online safety rules

- I will only use school IT equipment for activities when a trusted adult has given me permission and is present.
- I will not deliberately look for, save or send anything that could make others upset.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, 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 keep my username and password secure; this includes not sharing it with others.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- I will always use my own username and password to access the school network and subscription services such as; PurpleMash, Google Classroom, EdShed.
- In order to help keep me and others safe, I know that the school can check my files and the online sites that I visit. They will contact my parents / carers if an adult at school is concerned about me.
- I understand that everything I do or receive online can be traced now and in the future.
- I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- Before I share, post, or reply to anything online I will T.H.I.N.K
- T = Is it true?
- H = Is it helpful?
- I = Is it Inspiring?
- N = Is it necessary?
- K = Is it kind?
- I will not use my personal email address or other personal accounts in school or school email addresses at home.
- 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 open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- 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 in Year 6 mobile phones are allowed in school but other personal devices are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom
- 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.

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 electronic 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 Lead, Kate Hooft.

Please complete the form below to show that you agree to follow this Agreement:

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……..

Appendix F – Parent Carer Agreement

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.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.
(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with Kate Hooft. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils, and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school.
I/we understand that the school does not allow any events to be recorded on personal devices under any circumstances.
I/we understand that under no circumstance should images be taken, on personal devices, at any time on school premises.
I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.
We will ask parents and carers to confirm on an annual basis as to whether they give consent to images of their child being taken and used within school for specific purposes in line with the rest of this policy.
Should any parent wish to change their decision during the school year, they should contact the school.

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)…….

Parent/carer signature……..

Date ……...…..…

Appendix G - 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 through online training. 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 may only use personal mobile phones and devices in designated areas of the school. Under no circumstance should images be taken at any time on school premises. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

- 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 Kate Hooft 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 H - 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, head teacher) and staff members should seek support from their line manager or a senior member of staff.

- 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 head teacher 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 I - 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 F (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 head teacher 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 J - 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 Kate Hooft.

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 K - 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 Lead/DSL/ Headteacher	
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 L - Online safety incident log

Summary details of ALL online safety incidents will be recorded on this form by the Online Safety Lead or other designated member of staff. This incident log will be monitored at least termly, and info0072mation reported to SLT and governors.

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

Appendix M – Safeguarding and remote education during coronavirus (COVID-19)

Useful resources

Below are resources (please note not an exhaustive list) to help schools manage and risk assess any remote teaching and working.

Government guidance on safeguarding and remote education
https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

The Key for School Leaders - Remote learning: safeguarding pupils and staff
https://schoolleaders.thekeysupport.com/covid-19/safeguard-and-support-pupils/safeguarding-while-teaching/remote-teaching-safeguarding-pupils-and-staff/?marker=content-body

NSPCC Undertaking remote teaching safely
https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely

LGfL Twenty safeguarding considerations for lesson livestreaming
https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf

swgfl Remote working a guide for professionals
https://swgfl.org.uk/assets/documents/educational-professionals-remote-working.pdf

National Cyber Security Centre Video conferencing. Using services securely
https://www.ncsc.gov.uk/files/vtc_infographic.pdf