



Online Safety Policy

2021-2022

Head Teacher	Paul Griffin
Policy written by	Mandeep Mann
Policy approved by Governing Body	
Next review date	



Contents

1 Introduction and Overview

- 1.1. Rational
- 1.2. Policy Scope
- 1.3. Roles and Responsibilities
- 1.4. Monitoring and Review

2. Education and Curriculum

- 2.1. Education and Engagement with Pupils
- 2.2. Vulnerable Learners
- 2.3. Training and Engagement with Staff
- 2.4. Awareness and Engagement with Parents and Carers

3. Reducing Online Risks

4. Safer use of Technology

- 4.1. Classroom Use
- 4.2. Managing Internet Access
- 4.3. Filtering and Monitoring
- 4.4. Managing Personal Data Online
- 4.5. Security and Management of Information Systems
- 4.6. Password Policy
- 4.7. Managing the Safety of our Website
- 4.8. Publishing Images and Videos Online
- 4.9. Managing Emails
- 4.10. Managing the Learning Platforms

5. Social Media

- 5.1. Expectations
- 5.2. Staff Personal use of Social Media
- 5.3. Learners Personal use of Social Media

6. Use of Personal Devices and Mobile Phones

- 6.1. Expectations
- 6.2. Staff and Visitors use of Personal Devices and Mobile Phones
- 6.3. Pupils' use of Personal Devices and Mobile Phones

7. Responding to Policy Breaches

- 7.1. Concerns about Pupil Welfare
- 7.2. Staff Misuse

8. Procedures for Responding to Specific Online Incidents or Concerns

- 8.1. Youth Produced Sexual Imagery or "Sexting"
- 8.2. Online Child Sexual Abuse or Exploitation
- 8.3. Indecent Images of Children (IIOC)

9. Cyberbullying

10. Online Hate

11. Online Radicalisation and Exploitation

12. Links with other Policies and Practices



1. Introduction and Overview

1.1 Rational

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Park Hill Primary School with respect to the use of Computing-based technologies.
- Safeguard and protect the children and staff of Park Hill Primary School and comply with GDPR (General Data Protection Regulation).
- 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 the internet 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.
- Ensure that all members of the school community 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: being exposed to illegal, inappropriate or harmful material

Contact: being subjected to harmful online interaction with other users

Conduct: personal online behaviour that increases the likelihood of, or causes, harm

(Further explanations and examples can be found in Appendix 1.)

1.2 Policy Scope

Park Hill Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online. We believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online. This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as “staff” in this policy) as well as learners, parents and carers.

Park Hill Primary identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

1.3 Roles and Responsibilities

Park Hill Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety. The table below outlines the key responsibilities for members of the school community.

Role	Key Responsibilities
Leadership and Management Team	• Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements. • Ensure there are appropriate and up-to-date policies regarding online safety; including a Staff Code of Conduct and Acceptable Use Policy (AUP), which covers acceptable use of technology. • Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks. • Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety. • Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities. • Ensure parents are directed to online safety advice and information. • Provide information on a school's website for parents and the community. • Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support. • Ensure that appropriate risk assessments are undertaken regarding the safe use of technology. • Audit and evaluate online safety practice to identify strengths and areas for improvement.
Designated Safeguarding Lead (DSL)	• Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate. • Ensure all members of staff receive regular, up-to-date and appropriate online safety training. • Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up-to-date required to keep learners safe online. • Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online. • Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.



	• Work with staff to coordinate participation in local and national events to promote positive online behaviour. • Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches. • Report online safety concerns, as appropriate, to the Governing Body. • Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input. • Meet regularly with the governor with a lead responsibility for safeguarding.
Staff Members	• Contribute to the development of online safety policies. • Read and adhere to the Online Safety Policy and Acceptable Use Policy. • Take responsibility for the security of setting systems and the data they use or have access to. • Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site. • Embed online safety education in curriculum delivery, wherever possible. • Have an awareness of a range of online safety issues and how they may be experienced by the children in their care. • Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures. • Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally. • Take personal responsibility for professional development in this area. • Identify students who are involved in cybercrime, or those who are technically gifted and talented and are at risk of becoming involved in cybercrime and make a Cyber Choices referral.
Network Manager/Technician (Robin and Martin Ltd)	• Implement appropriate security measures as directed by the DSL and leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised. • Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team. • Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team • Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.



Parents and Carers	• Read the acceptable use policies and encourage their children to adhere to them. • Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home. • Role model safe and appropriate use of technology and social media. • Abide by the Acceptable Use Policy. • Identify changes in behaviour that could indicate that their child is at risk of harm online. • Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online. • Use our systems, such as learning platforms, and other network resources, safely and appropriately. • Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.
Learners (at a level that is appropriate to their individual age and ability)	• Engage in age-appropriate online safety education opportunities. • Contribute to the development of online safety policies. • Read and adhere to the Acceptable Use Policy. • Respect the feelings and rights of others both on and offline. • Take responsibility for keeping themselves and others safe online. • Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

1.4 Monitoring and Review

Park Hill Primary will review this policy and practices at least annually and following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure. We will ensure that we regularly monitor internet use; pupil's internet use will be monitored through teacher and teaching assistants whilst in their care, staff's internet use will be monitored through the filtering system and will be investigated further should anything be flagged up. We will evaluate online safety mechanisms to ensure that this policy is consistently applied. The DSL for each school and the DDSL team will be informed of online safety concerns, as appropriate. The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes. Any issues identified will be incorporated into the school's action planning.

2 Education and Curriculum

2.1 Education and Engagement with Pupils

Park Hill Primary will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The school will support learners to read and understand the Acceptable Use Policy (AUP) in a way which suits their age and ability by:

- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Implementing appropriate peer education approaches.
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

2.2 Vulnerable Learners

The school is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. Park Hill Primary will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils (see also SEND policy). The school will seek input from specialist staff as appropriate, including the SENDCo, Pastoral Manager and the SLT.



2.3 Training and Engagement with Staff

Park Hill Primary will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
 - This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that school systems are monitored, and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

2.4 Awareness and Engagement with Parents and Carers

Park Hill Primary recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies. We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, our Remote Learning Agreement.
- Requiring them to read our Acceptable Use Policy and discuss the implications with their children (where age appropriate).

3 Reducing Online Risks

Park Hill Primary recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.



- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our Acceptable Use Policy, Staff Code of Conduct and highlighted through a variety of education and training approaches.

4 Safer Use of Technology

4.1 Classroom Use

Park Hill Primary uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- TEAMS, ClassDojo and SharePoint
- Email
- Digital cameras, web cams and video cameras

All setting owned devices will be used in accordance with our Acceptable Use Policy and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.

Supervision of learners will be appropriate to their age and ability.

- Early Years Foundation Stage and Key Stage 1
 - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
- Key Stage 2
 - Learners will use age-appropriate search engines and online tools.
 - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

4.2 Managing Internet Access

The school will maintain a record of users who are granted access to the school's devices and systems. All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.



4.3 Filtering and Monitoring

Decision Making

- Park Hill Primary leadership have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

Filtering

- Education broadband connectivity is provided through Coventry City Council, and using the Impero Monitoring System.
- The school's filtering systems, Smoothwall, blocks all sites on the Internet Watch Foundation (IWF) list, which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- Robin and Martin Ltd (technical support) work to ensure that our filtering policy is continually reviewed.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, West Midlands Police or Child Exploitation and Online Protection Command (CEOP).

Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
 - Physical monitoring and supervision of the children using the devices
 - Monitoring internet and web access through the technology monitoring services provided by:
 - Impero Monitoring System
 - Smoothwall
- The school has a clear procedure for responding to concerns identified via monitoring approaches. Issues should be raised and will be responded to, by following the Child Protection procedures that are already in place.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.



4.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with the GDPR -Data Protection Act 2018. Full information can be found in the school's Data protection-GDPR Policy.

4.5 Security and Management of Information Systems

Park Hill Primary takes appropriate steps to ensure the security of our information systems including:

- Virus protection being updated regularly
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on the schools' networks.
- The appropriate use of user logins and passwords to access the school networks.
- All users are expected to log off or lock their screens/devices if systems are unattended.

4.6 Password Policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year Reception all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
 - Always keep their password private; users must not share it with others or leave it where others can find it.
 - Not to login as another user at any time.

4.7 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.



4.8 Publishing Images and Videos Online

The schools will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to): Data Protection-GDPR Policy, AUP, Staff Code of Conduct and Use of personal devices and mobile phones.

4.9 Managing Emails

Access to schools' email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: AUPs and Staff Code of Conduct.

- The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Email access on personal devices should be through the Outlook App and should require touch id or face recognition.

Members of the school community will immediately tell the DSL Team if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

Staff Email

- All members of staff are provided with a specific school email address, to use for all official communication. The use of personal email addresses by staff for any official school business is not permitted.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and parents.

Pupil Email

- Pupils will use provided email accounts for educational purposes.
- Learners will sign an AUP and Home School Agreement and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the setting.

4.10 Managing of Learning Platforms

Park Hill Primary using the learning platforms Microsoft TEAMS and ClassDojo.

- Only current members of staff, learners and parents will have access to learning platforms.
- When staff and/or learners leave the setting, their account will be disabled.
- Learners and staff will be advised about acceptable conduct and use when using the learning platforms.
- All users will be mindful of copyright and will only upload appropriate content onto the learning platforms.



- Any concerns about content on the learning platforms will be recorded and dealt with in the following ways:
 - The user will be asked to remove any material deemed to be inappropriate or offensive.
 - If the user does not comply, the material will be removed by the site administrator.
 - Access to the learning platforms for the user may be suspended.
 - The user will need to discuss the issues with a member of leadership before reinstatement.
 - A learner's parents/carers may be informed.
 - If the content is illegal, we will respond in line with existing child protection procedures.

5 Social Media

5.1 Expectations

- The expectations' regarding safe and responsible use of social media and remote learning platforms applies to all members of the Park Hill Primary School community.
- Members of staff will refer to and adhere to the schools Staff Handbook and Staff Code of Conduct where the staff use of social media is referred to.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
- Concerns regarding the online conduct of any member of Park Hill Primary's community on social media, should be reported to the DSL and will be managed in accordance with our Staff Code of Conduct, Behaviour and Child Protection Policies.

5.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Staff Code of Conduct within the AUP.
- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school's policies and the wider professional and legal framework.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.



- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.

5.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age-appropriate sites and resources. We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including Anti-bullying, Child Protection and Behaviour.
- The DSL (or DDSL) will respond to online safety concerns involving safeguarding or child protection risks in line with our Child Protection Policy.
- Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
 - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
 - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
 - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
 - To use safe passwords.
 - To use social media sites which are appropriate for their age and abilities.
 - How to block and report unwanted communications.
 - How to report concerns both within the setting and externally.

6 Use of Personal Devices and Mobile Phones

6.1 Expectations

Park Hill Primary recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

N.B. Electronic devices references to: mobile technology including mobile phones and personal devices such as tablets, e-readers, games consoles and wearable technology (including 'smart watches' and fitness trackers which facilitate communication or have the capability to record sound or imagery).

- Members of staff will refer to and adhere to the schools AUP and any other policy where the staff use of personal devices and mobile phones is referred to.



- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times. All members of the school community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
- All members of the school community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Staff Code of Conduct policy.
- All members of the school community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Child Protection Policies.

6.2 Staff and Visitor Use of Personal Devices and Mobiles

- Members of staff and visitors will ensure that use of personal phones and devices takes place in accordance with relevant school policy and procedures, such as: Child Protection, GDPR and AUP.
- Staff and visitors will be advised to:
 - Keep mobile phones and personal devices in a safe and secure whilst on the school site.
 - Keep mobile phones and personal devices switched off or switched to 'silent' mode during teaching time.
 - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
 - Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Staff and visitors will not use personal devices, such as: mobile phones, tablets or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, action will be taken in line with the school Staff Code of Conduct policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

6.3 Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Pupils' personal devices and mobile phones to be kept in a secure place designated by the school and switched off.
- Mobile phones or personal devices will not be used by pupils at any time during the school day.



- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place. It must be collected by the pupil's parents.

7 Responding to Policy Breaches

- All members of the community will be made aware of how the school will monitor policy compliance eg: AUPs, staff training, classroom management.
- All members of the community are informed of the need to report policy breaches or concerns in line with existing policies, including those mentioned in point 12. They will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the Whistleblowing procedure.
- We require staff, parents/carers and learners to work in partnership with us to resolve issues.
- If appropriate, after any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from Coventry Safeguarding Children's Partnership.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm.

7.1 Concerns about Pupil Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns. The DSL will record these issues in line with the school's Child Protection Policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies as outlined in the Child Protection Policy.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

7.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher/Chair of Governors, according to the Whistleblowing Policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Code of conduct.



8 Procedures for Responding to Specific Online Incidents or Concerns

8.1 Youth Produced Sexual Imagery or “Sexting”

- Park Hill Primary recognises youth produced sexual imagery (known as “sexting”) as a safeguarding issue; therefore all concerns will be reported to and dealt with by the DSL.
- Park Hill Primary will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of ‘sexting’ by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Dealing with “sexting”

- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will act in accordance with our Child Protection and Safeguarding Policies and the relevant Coventry Safeguarding Children’s Partnership procedures.
- The incident should be referred to the DSL as soon as possible.
 - The DSL should hold an initial review meeting with appropriate school staff to establish the facts and assess the risks.
 - There should be subsequent interviews with the young people involved (if appropriate).
 - Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm.
 - At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children’s social care and/or the police immediately.
- The DSL will follow the guidance from UKCIS with regards to the following actions:
 - Securing and handing over devices to the police
 - Searching devices, viewing and deleting imagery
 - Interviewing and talking to the young person/people involved
 - Recording incidents.

8.2 Online Child Sexual Abuse and Exploitation

- Park Hill Primary will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.



Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of incident involving online sexual abuse of a child, the school will act in accordance with the school's Child protection and Safeguarding policies and the Coventry Safeguarding Children's Partnership procedures.
 - Immediately notify the DSL.
 - Store any devices involved securely.
 - Immediately inform West Midlands Police via 101 (or 999 if a child is at immediate risk)
 - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
 - Inform parents/carers about the incident and how it is being managed.
 - Make a referral to Specialist Children's Services (if required/ appropriate).
 - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
 - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- If the school is unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Coventry Safeguarding Children's Partnership and/or West Midlands Police.
- If pupils at other schools are believed to have been targeted, the school will seek support from Coventry Safeguarding Children's Partnership and/or West Midlands Police first to ensure that potential investigations are not compromised.

8.3 Indecent Images of Children (IIOC)

- Park Hill Primary will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- Park Hill Primary will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list (via Coventry City Council) and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Coventry Safeguarding Children's Partnership and/or West Midlands Police.
- If made aware of IIOC, the school will:
 - Act in accordance with the schools Child Protection and Safeguarding Policy and the relevant Coventry Safeguarding Children's Partnership procedures.
 - Immediately notify the school DSL.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), West Midlands police or the LADO.



9 Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Park Hill Primary School. Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy.

10 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Park Hill Primary School and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Coventry Safeguarding Children's Partnership and/or West Midlands Police.

11 Online Radicalisation and Extremism

- The Federation will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carers may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with the Child Protection policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the Child Protection and Whistleblowing policies.

12 Links with other Policies and Practices

This policy links with a number of other policies, practices and action plans including:

Acceptable Use Policy	Child Protection Policy
Anti-bullying policy	Curriculum policies, such as: Computing Personal Social and Health Education (PSHE) Relationships and Sex Education (RSE)
Staff Handbook	Data Protection-GDPR Policy
Staff Code of Conduct	Image Use Policy
Behaviour Policy	Remote Learning Policy
SEND Policy	Whistleblowing Policy



Appendix 1

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

Content

- Ignoring age ratings while playing online games (exposure to violence associated with often racist/foul language, addiction, in-app purchases)
- Exposure to inappropriate content, including online pornography,
- Ignoring age restrictions on social networking websites such as Instagram, Facebook, YouTube, Snapchat, WhatsApp and other apps.
- Data breach
- Hate sites, sites inciting radicalisation and/or extremism
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft and sharing passwords

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)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)
- Inappropriate Messaging