Online Safety Policy

Berry Hill Primary School

Approved by:	The Governing body
Last reviewed on:	January 2026
Next review due by:	January 2027

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

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

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

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

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

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Magnus Wright.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated safeguarding lead

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

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy

- Ensuring that any online safety incidents are logged (see appendix 6) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4) contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting to ATOM IT.
- Following the correct procedures by contacting ATOM IT if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

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

3.7 The Online Safety Officer/Coordinator

The Online Safety Officer/Coordinator is responsible for:

- Leading the Online Safety Group and coordinating online safety work within school3
- Taking day-to-day responsibility for online safety issues and leading in establishing and reviewing the school online safety policies and documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Providing training and advice for staff on online safety matters
- Liaising with the Local Authority and other relevant bodies on online safety issues
- Liaising with school technical staff on online safety matters
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments
- Meeting regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Attending relevant meetings or committees of Governors
- Reporting regularly to the Senior Leadership Team on online safety matters
- Receiving regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations

This is not a technical role but focuses on raising awareness of online safety issues and coordinating online safety work within school. The role may be linked to safeguarding, behaviour and anti-bullying responsibilities.

3.8 The Online Safety Group

Berry Hill Primary School has established an Online Safety Group to provide a forum to look at all issues around online safety and to monitor the Online Safety Policy, including the impact of emerging issues.

The group includes representation from:

- Senior Leadership Team
- Online Safety Officer/Coordinator
- Teaching and support staff
- Technical staff
- Governing body
- Parents and carers (where appropriate)

The Online Safety Group is responsible for:

- Supporting the production, review and monitoring of the school Online Safety Policy and documents
- Supporting the production, review and monitoring of the school filtering policy and managing requests for filtering changes
- Mapping and reviewing the online safety curricular provision, ensuring relevance, breadth and progression
- Monitoring network, internet and incident logs
- Consulting stakeholders, including parents/carers and pupils, about the online safety provision
- Providing regular reporting to the Governing Body on online safety matters

3.9 Network Manager/Technical Staff

The Network Manager/Technical Staff are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements and any Local Authority or other relevant body Online Safety Policy and guidance that may apply
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network, internet, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher and Online Safety Coordinator for investigation, action or sanction
- That monitoring software and systems are implemented and updated as agreed in school policies
- Regular reviews and audits of the safety and security of school technical systems are conducted
- Servers, wireless systems and cabling are securely located and physical access is restricted
- That any online safety incidents are logged and dealt with appropriately in line with this policy
- That any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

3.10 Visitors and members of the community

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

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4.1 Building Resilience and Critical Thinking

As part of our online safety curriculum, pupils will also be taught:

- **Critical awareness of online content**: Pupils will develop the ability to critically evaluate the materials and content they access online and will be guided to validate the accuracy of information they find
- **Acknowledging sources**: Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- **Resilience to radicalisation and extremism**: In line with the Counter Terrorism and Security Act 2015, pupils will have opportunities to build resilience to radicalisation and extremist material by:
    - Participating in a safe environment for debating controversial issues
    - Understanding how they can influence and participate in decision-making
    - Recognising the dangers of extremist and terrorist material online
    - Knowing how to report concerning content

4.2 Planned Programme of Online Safety Education

Online safety is delivered through:

- A planned online safety curriculum as part of Computing, PSHE and other lessons, which is regularly revisited throughout the school year
- Key online safety messages reinforced as part of a planned programme of assemblies and pastoral activities

- Participation in national initiatives such as Anti-Bullying Week and Safer Internet Day
- Staff acting as good role models in their use of digital technologies, the internet and mobile devices

4.3 Supervised and Safe Internet Searching

When internet use is pre-planned in lessons:

- Pupils will be guided to sites that have been checked as suitable for their use
- Processes are in place for dealing with any unsuitable material that is found in internet searches
- Staff will be vigilant in monitoring the content of websites pupils visit

Where pupils may be allowed to search the internet more freely for educational purposes, staff will:

- Ensure appropriate supervision is in place
- Monitor the content of websites being visited
- Be aware that for good educational reasons, pupils may occasionally need to research topics (such as racism, drugs, or discrimination) that would normally result in internet searches being blocked

If such research is necessary:

- Staff can request that Technical Staff temporarily remove those sites from the filtered list for the period of study
- Any such request will be auditable with clear reasons documented for the need
- The temporary change will be time-limited and logged

5. Educating parents/carers about online safety

5.1 Communication with Parents/Carers

The school recognises that parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way.

The school will raise parents/carers' awareness of internet safety through:

- **Letters and communications home, including alerts made through Class Dojo**
- **Newsletters containing online safety tips and information about emerging risks**
- **Information on our website, including a dedicated Parent Zone with online safety resources**
- **Parent and carer events and workshops on online safety topics**
- **Participation in national campaigns such as Safer Internet Day, with information shared with families**
- **This policy, which is published on the school website and available on request**

5.2 Information Provided to Parents/Carers

On the school website and through other communications, the school will inform parents/carers about:

- **What systems the school uses to filter and monitor online use**
- **What their children are being asked to do online, including the sites they will be asked to access**
- **Who from the school (if anyone) their child will be interacting with online**
- **Current online safety issues and emerging trends that may affect their children**
- **Strategies for keeping children safe online at home**

5.3 Supporting Parents/Carers

The school will support parents and carers to keep up to date with emerging trends and potential online threats by:

- **Providing information about new technologies and platforms that children may be using**

- Sharing guidance on parental controls and safety settings
- Offering practical advice on having conversations about online safety with their children
- Signposting to reputable online safety resources and organisations

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

- What are the issues? – UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics – Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent resource sheet – Childnet International: https://www.childnet.com/resources/parents-and-carers-resource-sheet
- Thinkuknow – National Crime Agency: https://www.thinkuknow.co.uk/parents/
- Internet Matters: https://www.internetmatters.org/
- Net Aware – NSPCC: https://www.net-aware.org.uk/

5.4 Raising Concerns

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher, headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

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

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

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

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from a DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

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

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

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

If inappropriate material is found on the device, it is up to the safeguarding team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

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

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

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

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our acceptable use of ICT / Internet policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

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

Berry Hill Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Berry Hill Primary School will treat any use of AI to bully pupils in line with our anti-bullying policy.

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

7. Filtering and Monitoring

7.1 Statutory Requirements

In accordance with the Department for Education's statutory guidance "Keeping Children Safe in Education", the governing body and school leadership ensure that:

- We do all that we reasonably can to limit children's exposure to online risks through the school's IT systems
- The school has appropriate filters and monitoring systems in place and regularly reviews their effectiveness
- Filtering and monitoring systems are appropriate to the age range of our pupils, the number of pupils, how often they access the school's IT systems, and are proportionate in terms of costs versus risks
- The appropriateness of our filters and monitoring systems is informed in part by our risk assessments, including those required by the Prevent Duty
- We are careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding

7.2 Filtering Systems

Berry Hill Primary School uses filtering systems to:

- Block access to illegal content, particularly child sexual abuse images, using the Internet Watch Foundation CAIC list, which is actively employed by our broadband and filtering provider
- Block access to harmful and inappropriate content without unreasonably impacting on teaching and learning
- Filter content related to terrorist and extremist material, in line with the Counter Terrorism and Security Act 2015
- Provide differentiated filtering appropriate to the age and stage of our pupils

Our filtering systems:

- Are updated regularly to respond to new and emerging risks
- Block content across various categories including, but not limited to: pornography, violence, extremism, self-harm, and other age-inappropriate material
- Are monitored by the Network Manager/Technical Staff and Online Safety Coordinator
- Are not the sole responsibility of one individual

7.3 Monitoring Systems

The school has monitoring systems in place that:

- Regularly monitor and record the activity of users on the school's technical systems
- Alert designated staff to any concerning or inappropriate online activity
- Keep logs of internet use, which are regularly reviewed
- Allow the school to respond quickly to any safeguarding concerns that arise from online activity

All users are made aware in the Acceptable Use Agreements that their activity on school systems is monitored.

7.4 Managing Filtering and Monitoring

- The DSL takes lead responsibility for understanding the filtering and monitoring systems and processes in place
- The DSL works with the ICT manager (ATOM IT) to ensure appropriate systems and processes are in place
- Staff know who the DSL is and understand that they are responsible for the filtering and monitoring systems
- Staff know how to report if they need to bypass filtering and monitoring systems for educational purposes, or if the systems are not working effectively, by contacting ATOM IT
- All filtering and monitoring changes are logged and reviewed regularly by the Online Safety Group

7.5 Requests for Filtering Changes

There is a clear process in place for managing requests for filtering changes:

- Staff must submit requests in writing to the Online Safety Coordinator and Technical Staff
- Requests must include clear educational reasons for the change
- All requests are logged and auditable
- Where temporary changes are made (e.g., for research on sensitive topics), these are time-limited and closely supervised
- Filtering change logs are reviewed regularly by the DSL and Online Safety Governor

7.6 Review of Filtering and Monitoring

The effectiveness of our filtering and monitoring systems is reviewed:

- At least annually by the Governing Body, DSL, and Technical Staff
- Following any serious online safety incident
- When new risks or technologies emerge
- As part of the annual review of this Online Safety Policy

8. Mobile Technologies and Personal Devices

8.1 School-Owned Devices

Berry Hill Primary School provides some school-owned mobile devices (such as tablets and laptops) for educational purposes.

For school-owned devices:

- Devices are allocated to specific staff members or classes as determined by the Senior Leadership Team
- Use is permitted during school hours and, where appropriate, for school business outside of school hours
- All school-owned devices are subject to the school's filtering and monitoring systems
- Personal use of school-owned devices is not permitted unless explicitly authorised by the Headteacher
- All software, applications and settings on school-owned devices are managed by the school's Technical Staff
- Users must not download or install any software, applications or files without authorisation from Technical Staff
- All data stored on school-owned devices remains the property of the school
- Users must not store personal information on school-owned devices
- School-owned devices must be returned to the school when the user leaves or when requested
- Users may be liable for damage to school-owned devices if this results from misuse or negligence
- Staff using school-owned devices will receive appropriate training on their safe and effective use

8.2 Personal Mobile Devices - Pupils

As stated in Section 8 of this policy, pupils may bring mobile devices into school but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

Additional requirements for pupils' personal devices:

- Personal devices must be stored securely when not in use
- The school accepts no responsibility for loss, damage or theft of personal devices
- Personal devices brought into school remain the responsibility of the pupil and their parents/carers
- Pupils must not use personal devices to access the school's wireless network unless specifically authorised for educational purposes
- Taking photographs or videos on personal devices is strictly prohibited unless under direct supervision of a staff member for a specific educational purpose
- Any misuse of personal devices in school will result in confiscation and may lead to further disciplinary action in line with the school's behaviour policy

8.3 Visitors' Personal Devices

Visitors to the school are expected to:

- Keep personal devices on silent or switched off during their visit
- Not use personal devices to take photographs or videos on school premises unless specifically authorised
- Not use devices in areas where children are present unless authorised for a specific purpose
- Follow the same acceptable use expectations as staff

8.4 Management and Technical Considerations

The school will consider the following when managing mobile technologies:

- Network capacity and connection speeds
- The level of technical support available (or not available) for personal devices
- Security risks in allowing connections to the school network
- Insurance and liability arrangements
- Access to cloud services and data protection implications
- Charging facilities (not provided for personal devices)
- Regular review of mobile technology policies in light of emerging technologies

This mobile technologies policy will be reviewed annually as part of the overall Online Safety Policy review.

9. Use of Digital and Video Images

9.1 Overview

The use of digital and video images plays an important part in learning activities at Berry Hill Primary School. Pupils and staff use digital cameras, tablets and other devices to record evidence of activities in lessons and out-of-school events.

However, we recognise that digital images can remain on the internet forever and may cause harm or embarrassment to individuals in the short or long term. They could potentially be used to bully, threaten, groom or radicalise young people. It is important that pupils learn to take control of their own digital footprint and ensure it reflects them in a positive way.

9.2 Educating Pupils About Digital Images

Staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, pupils will be taught to recognise:

- The risks attached to publishing their own images on the internet, particularly on social networking sites
- The importance of considering how images may be perceived by others
- That images shared online can be copied, shared and manipulated by others without their knowledge or consent
- The potential impact of images on their future (education, employment, relationships)
- Their responsibility not to take, share, publish or distribute images of others without permission
- How to report concerning images they may encounter online

9.3 Permission for Use of Images

- Written permission from parents or carers will be obtained before photographs or videos of pupils are published on the school website, social media platforms, in the local press, or in any other public arena
- This permission is obtained when pupils join the school and is reviewed annually
- Parents/carers may withdraw consent at any time by notifying the school in writing
- The school respects the wishes of parents/carers and pupils who do not wish to have photographs taken or published

9.4 Parents/Carers Taking Images at School Events

In accordance with guidance from the Information Commissioner's Office:

- Parents and carers are welcome to take videos and digital images of their children at school events for their own personal use
- Such use is not covered by the Data Protection Act as it is for personal use
- To respect everyone's privacy and, in some cases, protection, these images:
    - **Must not** be published or made publicly available on social networking sites or any other online platform
    - **Must not** include comments on any activities involving other pupils in the images
    - Should only feature the parent/carer's own child where possible
- The school will inform parents/carers of these expectations before each event
- If the school becomes aware that images have been shared inappropriately, we will contact the parents/carers concerned and request that the images are removed

9.5 Staff Taking Images of Pupils

Staff and volunteers may take digital or video images to support educational aims, but must follow these guidelines:

- Images must only be taken on school-owned equipment (school cameras, tablets, school-issued phones)
- The personal equipment of staff must not be used to take images of pupils
- Staff must follow school policies concerning the sharing, distribution and publication of those images
- Staff must ensure pupils are appropriately dressed and not participating in activities that might bring the individuals or the school into disrepute
- Staff must obtain permission from the Online Safety Coordinator or Senior Leadership Team before taking images
- Images must be stored securely on school systems and deleted when no longer required
- Images must only be used for the purpose for which they were taken
- Staff must not take images for their personal use

9.6 Publishing Images

When publishing photographs of pupils, the school will:

- Select images carefully to ensure pupils are appropriately dressed and that images cannot be used inappropriately
- Ensure the activity shown does not bring the school or pupils into disrepute
- Comply with good practice guidance on the use of such images
- Not use pupils' full names anywhere on a website, blog or in association with photographs
- Not use pupils' names in image file names
- Obtain permission from pupils and parents/carers before publishing pupils' work

9.7 Storage and Retention of Images

- All images taken for school purposes will be stored securely on the school's network
- Images will only be accessible to authorised staff members
- Images will be retained in line with the school's data retention policy
- When images are no longer required, they will be securely deleted
- Images must not be stored on personal devices or removable media unless encrypted and authorised

9.8 Reporting Concerns

Any concerns about the use of digital or video images should be reported immediately to the DSL or Headteacher.

10. Data Protection and Information Security

10.1 Legal Framework

Personal data will be recorded, processed, transferred and made available according to current data protection legislation, which requires that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

10.2 School Responsibilities

Berry Hill Primary School will ensure that:

- We hold the minimum personal data necessary to enable us to perform our functions and will not hold it for longer than necessary for the purposes it was collected for
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data will be fairly obtained in accordance with privacy notices and lawfully processed
- We have a Data Protection Policy in place
- We are registered as a Data Controller for the purposes of the Data Protection Act
- Responsible persons are appointed and identified: Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out regularly

- We have clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage and cloud computing which ensure that such data transfer and storage meets the requirements laid down by the Information Commissioner's Office

10.3 Staff Responsibilities

All staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure, password-protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure, password-protected devices
- Do not share personal data with unauthorised people
- Keep passwords secure and do not share them with others
- Lock their computer screens when leaving their desks
- Do not leave sensitive data on desks overnight or when not in use

10.4 Use of Portable Devices

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must have approved virus and malware checking software installed and up to date
- The data must be securely deleted from the device once it has been transferred or its use is complete
- Portable devices should not be used to store personal data unless absolutely necessary
- If portable devices are used, they must be kept secure at all times and never left unattended
- Loss or theft of any device containing personal data must be reported immediately to the DSL and Headteacher

10.5 Transferring Data

- Personal data should not be transferred outside of the school unless it is encrypted or securely protected
- Staff should use secure file transfer systems provided by the school (such as ATOM IT secure systems)
- Personal data should never be sent via personal email accounts
- When sending sensitive data via email, it should be encrypted or password-protected
- Staff should consider whether it is necessary to send personal data or whether anonymised data would suffice

10.6 Cloud Storage

- The school uses approved cloud storage systems that meet data protection requirements
- Staff must only use approved cloud storage systems authorised by the school
- Personal cloud storage accounts (such as personal Dropbox, Google Drive) must not be used to store school data or information about pupils
- Parents/carers will be informed if cloud systems are used that involve storing or processing personal data about their children

10.7 Data Breaches

In the event of a data breach:

- The breach must be reported immediately to the DSL, Headteacher and SIRO
- The school will investigate the breach and assess the risk to individuals
- Where required, the breach will be reported to the Information Commissioner's Office within 72 hours
- Individuals affected by the breach will be informed where appropriate
- The school will take steps to prevent further breaches and will learn from the incident

11. Acceptable Use of the Internet and ICT Systems in School

11.1 General Principles

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see appendices). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and will restrict access through filtering systems where appropriate.

11.2 Monitoring of Internet Use

- All use of the school's internet and ICT systems is monitored and logged
- The school uses monitoring software to identify any concerning or inappropriate online activity
- Users should have no expectation of privacy when using school systems
- Monitoring is carried out in accordance with data protection legislation and for safeguarding purposes
- Users are made aware of monitoring through the Acceptable Use Agreements

11.3 Unacceptable Use

The school considers the following to be unacceptable use of ICT systems and the internet, whether in or out of school:

Illegal or inappropriate content:

- Accessing, creating, storing, linking to or sending pornographic material
- Accessing, creating, storing, linking to or sending material that promotes discrimination based on race, gender, religion, disability, sexual orientation or any other protected characteristic
- Accessing, creating, storing, linking to or sending threatening, harassing or bullying material
- Accessing, creating, storing, linking to or sending material that promotes or facilitates extremism or terrorism
- Using school systems to run a private business or for personal financial gain
- Accessing, creating or sharing any material that breaches copyright law
- Accessing, creating or sharing any material that breaches the Data Protection Act

Security and system misuse:

- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Deliberately attempting to access, or accessing, another person's account without permission
- Sharing usernames and passwords with others or allowing others to access school systems using your credentials
- Corrupting or destroying other users' data
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential or proprietary information (e.g. financial information, personal information, databases, computer or network access codes and passwords)
- Attempting to gain unauthorised access to restricted areas of the network or to restricted areas of websites
- Deliberately or recklessly damaging or misusing ICT equipment

Inappropriate communication and conduct:

- Sending communications that are offensive, harassing or of a bullying nature
- Using personal email, social networking, instant messaging or text messaging to carry out digital communications with pupils (staff only)
- Impersonating someone else online
- Creating, sharing or accessing material that could bring the school into disrepute or breach the integrity of the ethos of the school

Resource misuse:

- Downloading or uploading large files that hinder others in their use of the internet
- Using the internet for online gaming (unless for educational purposes)
- Using the internet for online gambling
- Using the internet for online shopping or commerce (unless for approved school purposes)
- Excessive personal use of the internet or school systems

11.4 Responding to Unacceptable Use

- Any incidents of unacceptable use will be dealt with in accordance with this policy and other relevant school policies (behaviour policy for pupils, staff disciplinary procedures for staff)
- The severity of the response will depend on the nature and seriousness of the incident
- Incidents will be logged and monitored
- Serious incidents may be reported to external agencies including the police
- Repeated or serious misuse may result in withdrawal of access to school ICT systems

More information is set out in the acceptable use agreements in the appendices.

12. Communications and Digital Technology

12.1 School Email Systems

The school provides email accounts for staff and, where appropriate, for pupils (KS2 and above).

For all users:

- The official school email service is safe, secure and monitored
- All users should be aware that email communications may be monitored
- Staff and pupils should only use the school email service to communicate with others when in school or on school systems

- Email should be written and checked carefully before sending, particularly if it includes sensitive or confidential information
- Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature to the DSL or Online Safety Coordinator
- Users must not respond to any such communication

For staff:

- Staff must use school email accounts for all school-related communications with pupils, parents/carers and other professionals
- Staff must not use personal email addresses for school-related communications
- Staff should be aware that email sent from school accounts represents the school and should maintain appropriate professional standards
- Staff should not send sensitive or confidential information via email unless it is encrypted
- Staff should ensure that any sensitive information is clearly marked as such

For pupils:

- Whole class or group email addresses may be used at KS1
- Individual school email addresses may be provided for pupils at KS2 and above for educational use
- Pupils will be taught about appropriate email etiquette and safe email use
- Pupils must only use school email accounts for educational purposes
- Pupils should not give their email address to anyone they do not know
- Pupils must report any suspicious or concerning emails immediately to a teacher

12.2 Professional Digital Communications

Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, learning platforms etc.) must be professional in tone and content.

Staff must:

- Communicate only through official (monitored) school systems
- Maintain professional boundaries at all times
- Not share personal contact details (phone numbers, email addresses, social media profiles) with pupils or parents/carers
- Not accept friend requests or follow pupils on personal social media accounts
- Not communicate with pupils via personal email, text messaging or social media
- Ensure all communication is transparent and could withstand wider scrutiny
- Consider whether communication is necessary and appropriate before sending

Staff must not:

- Use personal devices or accounts to contact pupils or parents/carers for school-related matters
- Share personal opinions about school matters, colleagues, pupils or parents/carers online
- Make any communication that could bring the school into disrepute
- Engage in any communication that could be interpreted as grooming or inappropriate

12.3 Use of Learning Platforms and Online Tools

The school uses various online learning platforms and tools to enhance education.

For all users:

- Users must only access platforms and tools approved by the school
- Users should follow the specific guidance provided for each platform
- Any concerns about the security or content of a platform should be reported immediately
- Users should not share login details or allow others to use their accounts
- Personal information should not be shared on learning platforms beyond what is necessary

12.4 Communication with Parents/Carers

The school will communicate with parents/carers through:

- Official school email accounts
- The school website
- Class Dojo and other approved communication platforms
- Letters sent home
- Phone calls from school phones

Parents/carers should:

- Use official school communication channels to contact staff
- Not expect staff to respond to emails or messages outside of school hours
- Ensure all communications are respectful and appropriate
- Not share staff personal contact details without permission
- Report any concerns about communications through appropriate channels

12.5 Video Conferencing and Live Streaming

Where the school uses video conferencing or live streaming (such as for remote learning or virtual events):

- Only approved platforms will be used
- Staff will receive training on the safe use of video conferencing tools
- Sessions will be supervised by school staff
- Privacy settings will be enabled to prevent unauthorised access
- Recordings will only be made with appropriate permissions and will be stored securely
- Pupils and staff should ensure appropriate backgrounds and settings are used
- Appropriate behaviour and dress code expectations apply during video calls
- Clear guidance will be provided to pupils and parents/carers on safe participation

13. Social Media

13.1 Overview

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. This includes social networking sites, messaging apps, online gaming platforms, and apps with social media elements.

Berry Hill Primary School recognises the numerous benefits and opportunities which a social media presence offers. However, there are also risks associated with social media use, especially around safeguarding, bullying and personal reputation. This section sets out how the school, its staff, pupils and community approach the use of social media.

13.2 Official School Social Media Accounts

Where Berry Hill Primary School operates official social media accounts, the following procedures will be followed:

Approval and Management:

- All official school social media accounts must be approved by the Senior Leadership Team before being created
- Official accounts will clearly identify themselves as representing Berry Hill Primary School
- At least two members of staff will be responsible for administering and monitoring each account
- Access passwords will be kept secure and changed regularly
- A named individual will be responsible for overall oversight of each account

Content Guidelines:

- All content posted must be appropriate for the school's audience and reflect the school's values
- Content will be checked and approved before posting where appropriate
- Images of pupils will only be posted with appropriate parental consent
- Pupils' full names will not be used in association with their photographs
- Personal information about pupils will not be shared
- The school will consider the permanence of content before posting (what is online stays online)

Code of Behaviour:

- Users of official school accounts will behave professionally and responsibly
- Posts will be polite, friendly and informative
- The school will not engage in contentious debates on social media
- Comments on school social media will be moderated appropriately
- The school reserves the right to delete comments that are inappropriate, offensive or breach this policy
- Users who post inappropriate comments may be blocked from the school's social media

Monitoring and Reporting:

- Social media accounts will be monitored regularly
- Social media accounts will be monitored regularly for comments and messages
- Any concerning comments or messages will be reported to the DSL immediately
- Systems are in place for reporting and dealing with abuse and misuse
- Incidents on school social media may be dealt with under school disciplinary procedures
- **Safeguarding:**
- Staff managing social media accounts will be vigilant for safeguarding concerns
- Direct messages to school accounts will be monitored by at least two staff members
- Any safeguarding concerns arising from social media will be dealt with in accordance with the school's child protection and safeguarding policy

13.3 Staff Personal Use of Social Media

- **Protecting Professional Identity:**
- As professionals who work with children and young people, staff must be clear about how to manage their own risk and behaviour online. The key consideration is protecting pupils, the school and the individual's reputation.
- **Staff must:**
- Ensure that personal social media accounts are set to private
- Regularly check and update privacy settings on all social media platforms

- Be aware that content posted online, even on private accounts, may become public
- Consider how any content they post online could affect their professional reputation or the school's reputation
- Ensure personal opinions are not attributed to Berry Hill Primary School or Nottinghamshire County Council
- Be aware that they may be held responsible for comments made by others on their social media if they do not take action to remove them
- **Staff must not:**
- Make any reference to pupils, parents/carers or school staff on personal social media accounts
- Post any images of pupils, school events, or school premises on personal social media accounts
- Accept friend requests or follow current pupils or parents/carers of current pupils on personal social media accounts
- Engage in online discussions on personal matters relating to members of the school community
- Post content that could bring the school into disrepute or damage the professional reputation of the school or its staff
- Use social media in a way that breaches the school's Staff Code of Conduct or other policies
- **Former pupils:**
- Staff should exercise professional judgement about whether to accept friend requests from former pupils
- Staff should consider the age of the former pupil and how long ago they left the school
- In all cases, staff should maintain professional boundaries and be aware that their conduct online may still reflect on the school
- **Where staff breach these guidelines:**
- The matter will be investigated in accordance with the school's disciplinary procedures
- Serious breaches may constitute gross misconduct and could result in dismissal
- The school may take legal action if staff conduct brings the school into serious disrepute

13.4 Pupils' Personal Use of Social Media

Education:

- Pupils will be educated about the safe and responsible use of social media through the curriculum
- Pupils will be taught to think carefully before posting content online and to consider the permanence of online content
- Pupils will be taught about privacy settings and how to protect their personal information online
- Pupils will learn to recognise and report inappropriate content or contact on social media

Expectations:

- Pupils are expected to follow the school's Acceptable Use Agreement in relation to social media, both in and out of school
- Pupils should not post any content that mentions the school, staff members, or other pupils in a way that could bring anyone into disrepute
- Pupils should not post any images or videos taken at school without permission
- Pupils should report any concerning content or contact to a trusted adult immediately

Where pupils misuse social media:

- Incidents will be dealt with in accordance with the school's behaviour policy

- Where incidents involve other pupils or members of the school community, these will be investigated appropriately
- Parents/carers will be informed of incidents and may be asked to support the school in addressing the issue
- Serious incidents may be reported to external agencies, including the police where appropriate
- The school may take action in relation to pupil conduct outside school where it affects the welfare of pupils or staff or could bring the school into disrepute

13.5 Parents/Carers' Use of Social Media

Expectations:

- Parents and carers are expected to behave in a reasonable and respectful manner when using social media
- Parents and carers should not post negative or defamatory comments about the school, its staff, pupils or other members of the school community on social media
- Concerns about the school should be raised through appropriate channels (speaking to the class teacher, headteacher, or following the school's complaints procedure) rather than posted on social media

Protecting the school community:

- Parents and carers should not share images or videos taken at school events on social media where other pupils are identifiable (see Section 9 on Use of Digital Images)
- Parents and carers should not post content that could identify vulnerable members of the school community
- Parents and carers should model good online behaviour for their children

Where parents/carers breach these expectations:

- The school will contact the parent/carer to request removal of the content
- In serious cases, the school may seek legal advice and may take legal action
- The school may restrict the parent/carer's access to school premises if their conduct poses a risk to staff or pupils

13.6 Monitoring of Public Social Media

- As part of active social media engagement, it is good practice to proactively monitor the internet for public postings about the school.
- The Online Safety Coordinator and senior staff will regularly monitor public social media for mentions of the school
- The school will respond to social media comments according to clear procedures that balance transparency with safeguarding
- Positive comments and engagement will be acknowledged where appropriate
- Negative comments will be assessed and, where appropriate, the individual will be invited to discuss their concerns through official channels
- Defamatory, abusive or threatening comments may be reported to the social media platform and, in serious cases, to the police

13.7 Review

- The school's use of social media for professional purposes will be checked regularly by the DSL and Online Safety Group to ensure compliance with school policies.

14. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from ATOM IT.

15. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policy on ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [staff disciplinary procedures / staff code of conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

15.1 Classification of Incidents

Incidents will be classified as either:

- **Illegal incidents** - requiring immediate referral to police
- **Inappropriate incidents** - requiring internal action and possibly external agency involvement

Illegal incidents include:

- Child sexual abuse images (including youth-produced sexual imagery/"sexting")
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Promotion of terrorism or extremism
- Other criminal conduct, activity or materials
- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child

If there is any suspicion that material contains child abuse images, or if there is any other suspected illegal activity, the incident must be reported immediately to the police. The device in question must be isolated and not examined further.

15.2 Procedure for Investigating Incidents

In the event of suspicion of misuse, all steps in this procedure must be followed:

Initial steps:

- Have **more than one** senior member of staff or volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported

- Conduct the procedure using a **designated computer** that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise
- Use the **same computer** for the duration of the procedure
- Ensure that relevant staff have appropriate internet access to conduct the procedure, but that the sites and content visited are closely monitored and recorded (to provide further protection)

Recording evidence:

- Record the **URL** of any site containing the alleged misuse
- Describe the **nature of the content** causing concern
- If appropriate, record and store **screenshots** of the content on the machine being used for investigation
- Screenshots may be printed, signed, dated and attached to an incident report form
- **EXCEPTION:** Do NOT take screenshots of images of child sexual abuse - halt monitoring immediately and refer to the police

Assessment and action:

- Once investigation is complete, the Senior Leadership Team and DSL will judge whether the concern has substance
- If it does, appropriate action will be taken, which could include:
    - Internal disciplinary procedures
    - Involvement by Local Authority or national/local organisations (as relevant)
    - Police involvement and/or action

Evidence trail:

- All steps taken must be documented to provide an evidence trail
- The completed incident report form should be retained for evidence and reference purposes
- This demonstrates that investigations were carried out for safeguarding purposes

15.3 Specific Actions for Different Users

For pupils:

The following are examples of inappropriate activities that may result in disciplinary action:

- Deliberately accessing or trying to access material that could be considered illegal
- Unauthorised use of non-educational sites during lessons
- Unauthorised or inappropriate use of mobile phone, digital camera or other mobile device
- Unauthorised or inappropriate use of social media, messaging apps or personal email
- Unauthorised downloading or uploading of files
- Allowing others to access the school network by sharing username and passwords
- Attempting to access the school network using another pupil's or staff member's account
- Corrupting or destroying the data of other users
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements following previous warnings or sanctions
- Actions which could bring the school into disrepute or breach the integrity of the school's ethos
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident

- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes copyright or the Data Protection Act

Sanctions for pupils will be applied in line with the school's behaviour policy and may include:

- Discussion with class teacher or member of the Senior Leadership Team
- Informing parents or carers
- Removal of internet or computer access for a period
- Banning of mobile phone use in school
- Internal exclusion
- Fixed-term exclusion
- Permanent exclusion (in the most serious cases)

For staff:

The following are examples of inappropriate activities that may result in disciplinary action:

- Deliberately accessing or trying to access material that could be considered illegal
- Inappropriate personal use of the internet, social media or personal email
- Unauthorised downloading or uploading of files
- Allowing others to access the school network by sharing username and passwords, or attempting to access the school network using another person's account
- Careless use of personal data (e.g., holding or transferring data in an insecure manner)
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal email, social networking, instant messaging or text messaging to carry out digital communications with pupils
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity of the school's ethos
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Breaching copyright or licensing regulations
- Continued infringements following previous warnings or sanctions

Sanctions for staff will be applied in accordance with the school's staff disciplinary procedures and may include:

- Verbal or written warning
- Disciplinary meeting with the Headteacher or Governors
- Removal of IT access privileges
- Suspension
- Dismissal (in cases of gross misconduct)
- Referral to Teaching Regulation Agency or other professional bodies
- Police involvement where appropriate

15.4 Reporting and Logging

- All online safety incidents must be logged using the school's incident reporting system (CPOMS)
- Incident logs will include: date, individuals involved, nature of incident, action taken
- The DSL will review incident logs regularly and report trends to the Senior Leadership Team and Governors
- Incident logs will inform future online safety developments and policy reviews

16. Sexting

16.1 Definition

"Sexting" refers to images or videos generated by children under the age of 18, or of children under the age of 18, that are of a sexual nature or are indecent. These images are also known as "youth produced sexual imagery" or "nudes and semi-nudes."

These images may be:

- Created and shared between young people
- Shared via mobile phones, tablets or other devices
- Shared on social media, messaging apps or other online platforms
- Shared with people the young person does not know

The creation and sharing of such images is illegal, even if the young person has created and shared an image of themselves.

16.2 School Approach

Berry Hill Primary School recognises that sexting is a safeguarding issue and all concerns will be dealt with in accordance with our child protection and safeguarding policy.

Key principles:

- The welfare of the child or young person is paramount
- Each case will be considered on its own individual merit
- A consistent approach is needed to protect young people, staff and the school
- Children and young people who have been involved in sexting incidents require support, not punishment
- Staff must never view, copy, print, share or save youth produced sexual imagery

16.3 If Staff Become Aware of an Incident

If a member of staff becomes aware that an incident of sexting may have taken place, they must:

DO:

- Report it immediately to the DSL
- Confiscate the device involved (if appropriate and safe to do so) without viewing the content
- Reassure the pupil that they are not in trouble and that they will be supported
- Document what they have seen or heard using the school's safeguarding procedures

DO NOT:

- View, copy, print, share or save the imagery
- Ask the young person to share or describe the imagery
- Investigate the incident yourself
- Delete the imagery from devices or online services
- Ask other pupils to delete imagery
- Say or do anything that could be perceived as blaming the young person

16.4 DSL Response

When the DSL is informed of an incident, they will:

1. **Hold an initial review meeting** to assess:
    - The nature of the incident (was it consensual or coerced?)
    - The ages of those involved
    - Whether there are any indicators of grooming or exploitation
    - Whether there are any concerns about capacity to consent
    - Whether the imagery has been shared more widely
    - Whether there are any aggravating factors (such as threats or pressure)
2. **Decide on the appropriate response**, which may include:
    - Managing the situation internally through pastoral support and safeguarding procedures
    - Involving parents/carers (unless this would put the child at greater risk)
    - Making a referral to Children's Social Care
    - Making a referral to the police
3. **Consider whether to view the imagery:**
    - Imagery will only be viewed if there is no other way to assess the risk
    - If imagery must be viewed, this will be done by the DSL (or deputy) and will be done in the presence of another member of staff
    - Any viewing will be documented, including reasons for viewing
    - If illegal imagery is confirmed, the police will be contacted immediately
4. **Support the young people involved:**
    - Ensure appropriate pastoral support is provided
    - Consider what education is needed to prevent further incidents
    - Monitor the situation to ensure no escalation or repeat incidents

16.5 Reporting to External Agencies

When to report to police: The DSL will report incidents to the police when:

- The incident involves an adult (over 18)
- There is reason to believe the young person has been coerced, blackmailed or groomed
- There are concerns about the capacity of the young person to consent
- The imagery involves violent or sexual acts beyond that which is considered usual for that developmental stage
- The imagery involves a child under 13
- The school is concerned about the immediate safety of a young person

When to report to Children's Social Care: The DSL will make a referral to Children's Social Care when:

- There are concerns about the welfare of a child or young person
- There are indicators of abuse, neglect or exploitation
- A child is at immediate risk of harm

16.6 Parental Involvement

Parents and carers will be informed at an early stage unless:

- Informing them would put the child at greater risk

- There are concerns that they may be involved in the incident
- The police or Children's Social Care advise that parents should not be informed at that stage

When parents are informed:

- The school will explain the incident sensitively
- The school will explain how the incident is being managed
- The school will provide information about sources of support for parents and their child

16.7 Education and Prevention

The school will help prevent sexting incidents through:

- Age-appropriate education about healthy relationships, consent and online safety as part of PSHE and computing curriculum
- Teaching children about the legal consequences of creating and sharing sexual imagery
- Helping children understand the emotional impact on those involved
- Teaching children how to report concerns
- Providing information to parents and carers about sexting and how to talk to their children about it

16.8 Further Guidance

The school's response to sexting incidents is informed by:

- UK Council for Internet Safety (UKCIS) guidance: "Sharing nudes and semi-nudes: advice for education settings working with children and young people"
- "Sexting in schools and colleges: responding to incidents and safeguarding young people" (UKCCIS)
- Keeping Children Safe in Education (Department for Education)

17. Training

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

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

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

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

18. Monitoring arrangements

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

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

19. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Mobile Phone acceptable use policy

Appendix 1: Student/Pupil Acceptable Use Agreement (KS2 pupils)

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

Keeping Safe Online:

- The school will check how I use devices and the internet to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

Using Computers and the Internet Sensibly

- I will only use devices, apps and sites that I am allowed to, and will check if I am unsure.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.

Berry Hill Primary School Pupil Acceptable Use Agreement

Once you have read and understood the Acceptable Use Agreement, please fill in the sections below to show you have agreed to follow them.

- I have read and understood the Acceptable User Agreement and agree to follow the rules in order to help support the safe use of computing at our school. I understand that if I do not follow any of these rules my use of ICT in school may be restricted.
- I understand that these rules also apply when I am out of school and involved in any behaviour which might affect the school or other members of the school.

Name:

Class:

Appendix 2: Student/Pupil Acceptable Use Agreement (Foundation/KS1 Pupils)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Appendix 3:

Staff (and Volunteer) Acceptable Use Agreement

Principles

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

Acceptable Use Terms

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- When I use my mobile devices (laptops/tablets/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

Declaration

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: _____

Signed: _____

Date: _____

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date:**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: Useful Websites and Resources For School Staff

UK Council for Child Internet Safety (UKCCIS) https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Child Exploitation and Online Protection Centre (CEOP) https://www.ceop.police.uk/Safety-Centre/

Think U Know (National Crime Agency) https://www.thinkuknow.co.uk/

- Provides resources for teachers including downloadable lesson plans for all age groups

South West Grid for Learning (SWGfL) https://swgfl.org.uk/

- 360 degree safe: Self-review tool for schools
- Online Safety BOOST toolkit

Childnet International https://www.childnet.com/

- Resources for teachers and parents
- Digizen: resources about digital citizenship

Internet Watch Foundation https://www.iwf.org.uk/

- Reporting illegal content online

UK Safer Internet Centre https://www.saferinternet.org.uk/

- Resources for Safer Internet Day
- Advice for parents and educators

National Online Safety https://nationalonlinesafety.com/

- Guides for parents on apps, games and platforms

BBC Own It https://www.bbc.com/ownit

- Advice and resources for children on managing online life

For Parents and Carers

Internet Matters https://www.internetmatters.org/

- Age-specific advice for parents

Net Aware (NSPCC) https://www.net-aware.org.uk/

- Reviews of social networks, apps and games

Parent Info https://parentinfo.org/

- Collaboration between Parentzone and CEOP

Common Sense Media https://www.commonsensemedia.org/

- Reviews and age ratings for apps, games, TV and films

Thinkuknow Parents https://www.thinkuknow.co.uk/parents/

For Children and Young People

Childline https://www.childline.org.uk/

- 0800 1111 (free, confidential helpline)

Thinkuknow https://www.thinkuknow.co.uk/

Childnet – Know IT All https://www.childnet.com/resources/know-it-all-for-primary/

Digizen https://www.digizen.org/

Report Harmful Content https://reportharmfulcontent.com/

BBC Own It https://www.bbc.com/ownit

Specific Issue Guidance

Cyberbullying:

- Anti-Bullying Alliance: https://anti-bullyingalliance.org.uk/
- Cyberbullying.org: https://www.cyberbullying.org/

Sexting:

- UKCIS guidance on sharing nudes and semi-nudes: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

Radicalisation and Extremism:

- Educate Against Hate: https://educateagainsthate.com/
- Let's Talk About It: https://www.ltai.info/

Mental Health and Wellbeing:

- Young Minds: https://www.youngminds.org.uk/
- Place2Be: https://www.place2be.org.uk/

Curriculum Resources

Thinkuknow Resources by Age Group:

- Jessie & Friends (ages 4-5)
- Lee & Kim's Adventure (ages 5-7)
- Hector's World (ages 5-7)
- Band Runner (ages 8-10)
- Play, Like, Share (ages 8-10)
- Jigsaw (ages 11-14)
- Exposed (ages 14+)

Childnet Resources:

- Digiduck's Big Decision (Foundation/KS1)
- Know IT All for Primary (KS2)

Common Sense Education https://www.commonsense.org/education/digital-citizenship

- Free digital citizenship curriculum

Google Be Internet Legends https://beinternetlegends.withgoogle.com/en_uk

- Free resources for KS2 pupils

Audit and Assessment Tools

360 degree safe https://360safe.org.uk/

- Free self-review tool for schools
- Includes action planning and comparison with other schools

Online Safety BOOST https://boost.swgfl.org.uk/

- Incident management tool
- Policy templates and resources

Local Support

Nottinghamshire Safeguarding Children Partnership https://www.nottinghamshire.gov.uk/nscp

- Local safeguarding procedures and guidance

Nottinghamshire County Council Online Safety Support

- Contact through school's normal LA channels

Appendix 6: Online Safety Incident Report Log

Reporting Log

Group: _____

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		