Barlborough Primary School

Online Safety

Policy Document

Key Details

Designated Online Safety Lead: Miss E Jolly

Designated Safeguarding Lead (s): Kerry Towndrow-Birds

Named Governor with lead responsibility: Duncan Haywood

Date written: October 2020

Date agreed and ratified by Governing Body:

Date of next review: October 2021

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures

Contents of Barlborough Primary School's Online Safety Policy

1. Policy Aims

Our online safety Policy has been written by Barlborough Primary School, involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input, and reformatted including additions, with permission by the Child Protection Manager for Schools/Education, Derbyshire County Council as required. .

• It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2018, Early Years and Foundation Stage 2017, 'Working Together to Safeguard Children' 2018 and the Derbyshire Safeguarding Children Board procedures.

- The purpose of Barlborough Primary School's online safety policy is to:
  - Safeguard and protect all members of Barlborough Primary School's community online.
  - Identify approaches to educate and raise awareness of online safety throughout the community.
  - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
  - Identify clear procedures to use when responding to online safety concerns.

- Barlborough Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
  - **Content:** being exposed to illegal, inappropriate or harmful material for example, pornography, fake news, racist or radical and extremist views.
  - **Contact:** being subjected to harmful online interaction with other users for example,
  - commercial advertising as well as adults posing as children or young adults.
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm for
  - example, making, sending and receiving explicit images, or online bullying.

Online safety messages that are shared with staff, children and parents/carers at Barlborough Primary School will be appropriate and up-to-date and reflect the full range of risks; content, contact and conduct. The advice will empower them to be able to respond to a range of online threats as well as opportunities.

2. Policy Scope

- Barlborough Primary School believes that online safety is an essential part of safeguarding and acknowledges it's duty to ensure that all learners and staff are protected from potential harm online.

- Barlborough Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Barlborough Primary School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and/or the Code of conduct
    - Remote Learning Policy
    - Behaviour and discipline policy
    - Child protection policy
    - Confidentiality policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
    - Data security
    - Image use policy
    - Searching, screening and confiscation policy

2.3 Current and Emerging Internet Uses Within The Community

At Barlborough it is important to keep up to date with the current internet trends that pupils have access to outside school. The following are those which we have noted to be popular and therefore aim our Online Safety Teaching towards (as well as addressing all other aspects of Online safety education within the curriculum)

Apps and Websites

- Youtube- watching and in some circumstances creating content.
- Instant messaging via Whats App, Snap Chat or Instagram messenger.
- TikTok music video creator and publishing website/ social media platform.

- Online chat rooms- Particularly when online gaming
- Online gaming- Popular games are Fortnite, Pubg, Roblox, Animal crossing, and Call of Duty,
- Social networking sites -Snapchat, Instagram, Facebook and Twitter.
- Blogs and Micro-blogs -Twitter
- Video conferencing- Zoom, Microsoft Teams, FaceTime and Skype.
- Geocaching- Local 'treasure hunts' using GPS.
- Livestreaming (watching and conducting) via Youtube, Instagram and Twitch.

Devices

•Mobile phones with camera and video functionality
• Tablets and Ipads
• Smart Watches
• Laptops
• Games consoles- particularly Xbox, PS4, Wii and Nintendo Switch.

3. Monitoring and Review

- Barlborough Primary School will review this policy at least annually in order to keep it relevant to issues and regulations introduced in accordance with the rapid changes of the internet.
    - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, Mrs-Towndrow Birds will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

It has been discussed with staff, agreed by the senior management and approved by Governors. It will be reviewed annually
It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.
This Policy document is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

4. Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school to ensure children use the internet responsibly on the premises and at home and are aware of the risks that the internet brings as well as how to deal with these if they occur. The Designated

Safeguarding Lead (DSL) Kerry Towndrow-Birds, Head teacher, has lead responsibility for online safety within Barlborough Primary school.

- The school has appointed Miss Emma Jolly to be the online safety lead.
- Barlborough Primary School also recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff Code of conduct and/or an AUP, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.

- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.

- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.

- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.

- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet every term with the governor with a lead responsibility for safeguarding and online safety.
- Meet and lead online safety group meetings termly to monitor incidents, maintain and update policies, organise event and promote online safety in school and the wider community.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and AUPs which are updated annually.
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures *(including password policies and encryption)* to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team

- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.5 It is the responsibility of learners (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the school AUPs.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the school AUPs and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and/or AUPs.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies.
- Use school systems, such as Class Dojo and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.
- Seek information in regard to Online Safety which is regularly added to the School website such as the #Ditto magazine.
- Read information sent home informing them of updates and news which is often influenced by Derbyshire's 'Get safe online' scheme.
- Try to attend information evenings and workshops concerning Online Safety.

5. Education and Engagement Approaches

The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

5.1 Education and engagement with pupils

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:.
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in the PSHE, RSE and Computing programmes of study, covering use both at home school and home
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The school will support learners to read and understand the AUP in a way which suits their age and ability by:
    - Displaying acceptable use posters in all rooms with internet access.
    - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
    - Rewarding positive use of technology by pupils.
    - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
    - Seeking learner voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.

5.2 Vulnerable Pupils

- Barlborough Primary School is aware that some learners are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Barlborough Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- We will provide staff and parents with information taken from the publication “Learning disabilities, Autism and Internet safety” by MENCAP so that individual provision can be put in place at home and at school for children with SEN.
- Barlborough will ensure that 1:2:1 support is given to those who are deemed vulnerable, SEND, EAL or experiencing trauma or loss when using the Internet.
- Barlborough Primary School will seek input from specialist staff as appropriate, including the SENCO, Child in Care Lead and the Ed Psych.

- Children with SEND will use devices which have accessibility filters to ensure that they only access relevant apps.
- Filtering systems will also ensure that our Spanish and Romanian speaking pupils can access the Online Safety Education taught at Barlborough Primary School.

5.3 Training and engagement with staff

The school will:

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

5.3 Awareness and engagement with parents and carers

- Barlborough Primary school recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - Drawing their attention to the school online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information as part of joining our school, for example, within our home school agreement.
    - Requiring them to read the school AUP and discuss its implications with their children annually.

6. Reducing Online Risks

- Barlborough Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- Barlborough Primary School uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which includes search engines and educational websites
    - School learning platform/intranet
    - Email
    - Tablets
    - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place.
- Teacher tablets will only be used by members of staff and have an automatic lock screen with password protection on.
- Ipads will have 'guided access' switched on in order to ensure children are limited to what they access.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools *such as SWGfL Squiggle, Dorling, Google Safe Search or CBBC safe search*, following an informed risk assessment, to identify which tool best suits the needs of our community.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.
    - **Early Years Foundation Stage and Key Stage 1**
        - Learners access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials via the ipads and interactive whiteboards, which supports the learning outcomes planned for the pupils' age and ability.
        - Learners will use age-appropriate search engines and online tools.
    - **Key Stage 2**
        - Learners will use age-appropriate search engines and online tools.
        - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.
    - **Pupils in residential provision**
        - The school will balance children's ability to take part in age appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).

7.2 Managing Internet Access

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

7.3 Filtering and Monitoring

7.3.1 Decision Making

- Barlborough Primary School governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- The school uses educational broadband connectivity through the EMPSN framework and our supplier is KCom

- The school uses the Netsweeper filtering system which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. To date all categories listed in the IWF list are blocked the school has no exceptions to these categories. The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

- The school works with Netsweeper to ensure that our filtering policy is continually reviewed.

Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches.
    - If pupils discover unsuitable sites, they will be required to turn off monitor/screen and immediately report the concern to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Police or CEOP.

7.3.4 Monitoring

- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
    - The schools 2 technicians will review logfile information regularly and report it if needed. Logfile information will detail websites access and search term usage. Through regular monitoring, this information could enable schools to identify and intervene with issues concerning access or searches.
- The school has a clear procedure for responding to concerns identified via monitoring approaches. They will be logged on an 'Incident log sheet' and then given to Mrs Town-Bird (DSL) who will respond in line with the child protection policy and act appropriately.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 1998.
    - Full information can be found in the schools information security policy.

7.5 Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Regularly checking files held on the school's network,
    - The appropriate use of user logins and passwords to access the school network.
    - Specific user logins and passwords will be enforced for all but the youngest users or those which have specific provision due to SEND.
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - The Technical network manager will review system capacity regularly.
    - The school Internet access will be designed to enhance and extend education.
    - Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
    - Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the ICT Administrator

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.

- From year 3, all learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.

- We require all users to:
    - Use strong passwords for access into our system.
    - Change their passwords every half term or if they feel their login is known to others.
    - Always keep their password private; users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.

7.6 Managing the Safety of the School Website

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

7.7 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): the Image use policy, Data security, AUPs, Codes of conduct, Social media and Use of personal devices and mobile phones.

7.8 Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of conduct/ behaviour policy.
    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the SLT if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted to specific lessons only; access to external personal email accounts will be blocked on site.

- Barlborough has a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff. The email address is as followed; **onlinesafety@barlborough.derbyshire.sch.uk**

7.8.1 Staff email

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

7.8.2 Learner email

- Learners will use school provided email accounts for educational purposes.
- Learners will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Educational use of Videoconferencing and/or Webcams

- Barlborough Primary School recognise that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
    - Videoconferencing contact details will not be posted publically.
    - School videoconferencing equipment will not be taken off school premises without prior permission from the DSL.
    - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.
    - Staff will integrate lessons concerning safety when conducting videoconferencing or when creating content which could be published (outside of school) linking these to popular websites and apps which utilise similar skills such as Youtube, musically, twitch, snapchat and Instagram.

7.9.1 Users

- Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Learners will ask permission from a teacher before making or answering a videoconference call or message.

- Videoconferencing will be supervised appropriately, according to the pupils' age and ability. This will be outlined on an informal risk assessment conducted by the class teacher prior to the lesson and this will be approved by the Headteacher.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, the school will check that recording is permitted to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-school site, staff will check that the material they are delivering is appropriate for the class.
- Content produced should not be published on any video hosting websites such as Youtube or Vimeo.

7.10 Management of Learning Platforms

- Barlborough Primary School uses Class Dojo as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, including, message and communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff and/or pupils' leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Pupils and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A learners parent/carer may be informed.
    - If the content is considered to be illegal, then the school will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

7.11 Management of Applications (apps) used to Record Children's Progress

- The school uses Insight to track learners progress and share appropriate information with parents and carers.
- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, , and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
    - School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Barlborough Primary School's community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Barlborough Primary School's community are expected to engage in social media in a positive, safe and responsible manner, at all times.
    - All members of Barlborough Primary School's community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control learner and staff access to social media whilst using school provided devices and systems on site. Staff will plan in specific times when children can access blogs and Wikis and they will not be permitted to access these outside of the lesson hours without teacher permission.
    - The use of social media during school hours for personal use by staff is permitted at lunch time only on personal devices when children are not present or could potentially be present.

    - Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Barlborough Primary School's community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child protection policies.

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the AUP.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school.
- Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites as strictly as they can.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of Barlborough Primary School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
    - Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Headteacher.
    - If ongoing contact with learners is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.

8.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding learners use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media site, games or tools.
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications and report concerns both within school and externally.

8.4 Official Use of Social Media

- Barlborough Primary School's official social media channel is Facebook.
- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes in the Reception Class.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
    - Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use school provided email addresses to register for and manage any official school social media channels.
    - Official social media sites are suitably protected.
    - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Confidentiality and Child protection.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents, carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels by continuing to use other communication systems in place such as Teachers2Parents texting and Class Dojo.

Staff expectations

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
    - Sign the school's Social media acceptable use policy.
    - Be professional at all times and aware that they are an ambassador for the school.
    - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
    - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
    - Ensure that they have appropriate written consent before posting images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, learners.

- Inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

9. Use of Personal Devices and Mobile Phones

- Barlborough Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within school. When referring to devices such as (but not limited to)phones, smart watches, portable music devices and tablets.

9.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-bullying, Behaviour and Child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
  - All members of Barlborough Primary School's community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
  - All members of Barlborough Primary School's community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as toilets accessed by the children and areas of the school with children present. We recommend that the staff room or photocopier room is used if mobile phones and personal devices are needed.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of Barlborough Primary School's community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child protection, Data security and Acceptable use.
- Staff will be advised to:

    - Keep mobile phones and personal devices in a safe and secure place during lesson time for example in the staff room or in your bags locked in a secure cupboard.
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless written permission has been given by the Headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the Headteacher.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
    - Directly with learners and will only use work-provided equipment during lessons/educational activities.
    - Staff may not use portable storage devices to store work, however if they require to do so, must seek Miss Towndrow-Birds permission first and only use a device which is encrypted and have the password protection enabled at all times.
- If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy as well as our code of conduct.
    - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Learners Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Barlborough Primary School expects learners personal devices and mobile phones to be switched off and handed into the office on arrival through the gates.
- If a learner needs to contact his/her parents or carers they will be allowed to use a school phone in the office when staff are present.
    - Parents are advised to contact their child via the school office during school hours; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.
- Mobile phones or personal devices will not be used by learners during lessons or formal education time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
    - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
    - If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.

- Mobile phones and personal devices must not be taken into examinations.
    - Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a learner breaches the school policy, the phone or device will be confiscated and will be held in a secure place.
    - School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting).
    - Searches of mobile phone or personal devices will only be carried out in accordance with the school's policy.
    - Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes school policies.
    - Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.
    - If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Child protection and Image use.
- The school will ensure appropriate signage and information is provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

9.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required, such as during residential trips.
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the Acceptable use policy and other relevant policies

10. Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
    - Learners, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.

- The school requires staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Learners Welfare

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

10.2 Staff Misuse

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

11. Procedures for Responding to Specific Online Incidents or Concerns

Any incident which occurs within school or outside of school will be logged and dealt with accordingly. These logs will be monitored regularly by the Online Safety Group and SLT. Parents will be informed of how each individual case is managed, with regular updates about the progress of it or if it has been closed.

11.1 Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.
- Barlborough Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- Barlborough Primary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Barlborough Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Barlborough Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.

        - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Derbyshire Police first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery or "Sexting"

- Barlborough Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead, Online Safety Lead and Headteacher.
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- Barlborough Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods such as those included on the ThinkuKnow website and those included in the SWGFL Digital Literacy Scheme.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

Dealing with 'Sexting'

- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
    - Act in accordance with our Child protection and Safeguarding policies.
    - Immediately notify the Designated Safeguarding Lead.
    - Store the device securely.
        - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
    - Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - Make a referral to Specialist Children's Services and/or the Police, as appropriate.
    - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
    - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
        - Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

    - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school will not:
    - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
        - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
    - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Barlborough Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Barlborough Primary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community. This is included on the website, on posters displayed in every classroom and on displays.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
    - Act in accordance with our child protection policies and the relevant Derbyshire Safeguarding Child Board's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Derbyshire police via 101, or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Team and/or Derbyshire Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy).
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Derbyshire Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- Barlborough Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Derbyshire Police and/or the Education Safeguarding Team.

- If made aware of IIOC, the school will:
    - Act in accordance with the schools child protection and safeguarding policy and the relevant Derbyshire Safeguarding Child Boards procedures.
    - Immediately notify the school Designated Safeguard Lead.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Derbyshire police or the LADO.

- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
    - Ensure that the Designated Safeguard Lead is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the school devices, the school will:

- Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
  - Ensure that the Headteacher is informed.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
  - Quarantine any devices until police advice has been sought.

11.4 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Barlborough Primary School.
- Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy which can be found http://www.barlborough.derbyshire.sch.uk/website/w308/file/repository/BPS_Anti_Bullying_Policy_policy_Jan_17.pdf
- Any incidents related to cyberbullying will be logged and managed by the Online Safety Leader.

11.5 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Barlborough Primary School and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- Any incidents related to online hate will be logged and managed by the Online Safety Leader, DSL and Anti-Bullying Lead.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Derbyshire Police.

11.6 Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.

- To ensure that the internet is not used to promote and/or research pro extremist or radicalisation material we will continuously monitor pupils internet content usage at school and report any suspicious incidences in accordance with the Tackling extremism and radicalisation policy introduced in 2015.
- Our filtering system is constantly updated to ensure no access can be gained to such sites on the school premises.
- Online lessons will also tackle these issues using current and up to date resources.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies.

11.8 Upskirting

The Voyeurism (Offences) Act, which is commonly known as the Upskirting Act, came into force on 12 April 2019. 'Upskirting' is where someone takes a picture under a persons clothing (not necessarily a skirt) without their permission and or knowledge, with the intention of viewing their genitals or buttocks (with or without underwear) to obtain sexual gratification, or cause the victim humiliation, distress or alarm. It is a criminal offence. Anyone of any gender, can be a victim. Staff at Barlborough Primary School have had recent training concerning this. If this occurs staff must do the following:

- Any incidents related to upskirting will be logged and managed by DSL.
- All members of the community will be advised to report upskirting in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Derbyshire Police

12. Using technology to facilitate home learning

As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, the DSL, school technician, governing bodies and proprietors at Barlborough Primary School will ensure appropriate filters and appropriate monitoring systems are in place in order to do this. Details of these are outlined in the Remote Learning Policy.

12. Useful Links for Educational Settings

Derbyshire Support and Guidance

Derbyshire County Council Education Safeguarding Team:

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
    - esafetyofficer@Derbyshire.gov.uk Tel: 03000 415797
- Guidance for Educational Settings:
    - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
    - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
    - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
    - Derbyshire e–Safety Blog: www.Derbyshireesafety.wordpress.com

KSCB:

- www.kscb.org.uk

Derbyshire Police:

- www.Derbyshire.police.uk or www.Derbyshire.police.uk/internetsafety
- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Derbyshire Police via 101

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
    - ChildLine: www.childline.org.uk
    - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
    - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

Online Safety Policy Summary

Using The Internet and Technology Safely in the Classroom at Barlborough Primary School

- School devices are only to be used at Barlborough Primary School as these have appropriate filters applied at device level or across the school internet.

- Staff must guide pupils to appropriate sites - you may consider selecting sites for younger pupils or discussing with older ones what content they may be looking for when carrying out an online search.

- All staff and volunteers must model good behavior when using ICT equipment and the internet.

-Staff should consider the pupil's privacy when sharing their images online. Regardless of whether you have obtained media consent, model best practice by asking their permission before posting an image of them online.

- All staff, learners and parents must act according to the Acceptable Use Policy when using ICT equipment or the internet. Teaching Staff should keep referring to this during Online Safety Lessons to familiarise themselves and their learners with these rules frequently.

Young People Viewing Content In Your Care

- Staff and visitors to Barlborough Primary School must check online content prior to the lesson by fully exploring any webpages which may be shown in class or by watching videos in their entirety. They will also have to make sure these are accessible on the school network with our filtering system.

- Staff should check search results first by performing a 'dry run' prior to the lesson to ensure the content displayed is appropriate.

- Staff should apply safety modes where available by using the settings of the site/ app to filter the content they search for. (Google offer a 'safe search' setting which can be found in the top right corner and YouTube offer a 'safety mode' which can be found at the bottom of the screen or within the settings of the app.)

- Where necessary staff should include possible online risks when completing risk assessment forms.

Our Online Safety Curriculum

-Online safety messages should be embedded in all areas of the curriculum by every member of staff at Barlborough Primary school. Staff should ensure that learners are reminded of online safety messages whenever using technology and the internet.

- A lesson dedicated to online safety should occur at the start of each half term and follow the SWGLF lesson plans.

- Staff should use a range of resources/ teaching methods in online safety lessons- there are a wealth of online resources to support you in delivering online safety messages in a range of ways. You may wish to use our 'Online Safety in the Computing Curriculum' guide to resources for suggestions—www.childnet.com/ resources/online-safety-and-computing

- Staff and Parents should stay up-to-date with technology and online content as it rapidly changes. Staff should ensure that they are teaching about the current risks and trends by researching or speaking to pupils. Parents will be educated on these matters through half termly newsletters, workshops and also contents added on Classdojo or the website when key information to support Online Safety.

- Staff should give advice about what to do in different online scenarios and teach them about the different routes to get help so that learners know what to do if something goes wrong online. This could include speaking to an adult, filling in Barlborough Primary School's incident form, saving evidence, reporting content on the website/app or via CEOP or contacting a helpline for support.

What Does Barlborough Primary School Do to Ensure Best Practice?

-We review this policy regularly and ensure the school's policy and AUP is up to date and has been shared/ communicated with all members of the school community.

-We have clear procedures in place to support online safety concerns and incidents, eg where a pupil has misused technology and the internet on purpose or by accident. These include the Incident logs, incident email address, weekly drop in sessions and seeking support from the DSL where necessary.

-An online safety group is set up which enables learners, parents, DSl, governors and members of the wider community to work together to monitor incidents, gather learner's feedback, educate other learners, parents and staff, plan events to celebrate Online Safety and take part in lessons within school.

-We use the free 360° safe online self-review tool to regularly self-assess our practice and approach to Online Safety.

- Staff only use appropriate methods of contact to communicate with parents. This will be through school channels such as Class Dojo, teachers 2 parents or phone calls using the school system.

- All devices in school have up to date firewalls and safety modes in place and are secured with passcodes.

- Filtering and monitoring systems are updated regularly and monitored by Duncan Smith, the ICT technician.

- Learners opinions and knowledge is highly valued at Barlborough Primary school and we gather this regularly to update out policies, feed into our Online Safety Planning and allow staff to develop their own knowledge about up to date affairs. We regularly conduct pupil surveys and questionnaires to gather this as well as through discussions within the Online Safety group.

Securing Our Content in School

- Pin/passcode on all devices (including staff laptops) will always be set up with a strong pin/passcode lock to ensure personal data and images are secure.

- Strong passwords will be used to secure data on the school server and staff laptops. These will include a mixture of lower and upper case letters, symbols and numbers to make it stronger. These will also be changed regularly and not given out to anyone in order to keep data secure at all times.

- Staff and learners must always log out of online accounts or desktop devices when leaving a device or the room in order to secure content.

How We Use and Store Photos of Young People At Barlborough Primary School

- We obtain consent before videoing or photographing pupils and ensure that all staff and visitors are clear about the school's policy and refer back to the relevant consent forms which have been completed by parents and carers.

- Staff will only use school devices when capturing images or videos of students.

-In accordance with GDPR regulations we consider where images and videos will be stored and how long for. We save files on our secure school network and delete these when they are no longer required or children have left the school.

What We Do When an Incident is reported

- We talk to those involved and fill in an incident log. (These will then be shared with DSL and adults involved in the Online safety group to monitor and follow up)

- We will screenshot or print out all content linked to the incident and keep a record of any incidences you are unable to capture content of.

- We will talk to parents and carers and inform them of any incidents which have occurred.

- We understand that ever incident is unique and try to resolve it sensitively and quickly.

Please note this is just condensed version of the full Online Safety Policy which must also be read. Each section included in this summary can be found in more detail within the policy itself and should be referred to when necessary.

Barlborough Primary School Declaration

Barlborough Primary School
Declaration

We confirm that this document is the school's official policy on Online Safety.

Headteacher:

_____

Name Kerry Towndrow-Birds

_____

Governor:

_____

Name:

_____

Date:

_____