Online Safety Policy

UPDATED: February 2021

REVIEW DATE: February 2022

Imagine, Believe, Achieve

Document name	Online Safety Policy
Document owner	Matlock Bath Holy Trinity Church of England (VC) Primary School
Authors	The education people, Kent County Council, Derbyshire County – CPM Schools/Education *Miss S Rouke*
Date approved & rectified	February 2021 (tbc)
Review date	February 2022
Head teacher/Principal	Mrs Sally Swain
Link Governor	Mr Nick Whitehead

Matlock Bath Holy Trinity CofE Primary School

Online Safety Policy

Designated Safeguarding Lead (s): Mrs Swain, Headteacher

Named Governor with lead responsibility: Nick Whitehead

Contents

Policy Aims

- This online safety policy has been written by Matlock Bath Holy Trinity CofE Primary School involving staff, learners and parents/carers, building on Kent County Council/The Education People online safety policy, 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', Early Years and Foundation Stage, 'Working Together to Safeguard Children' and the Derby City & Derbyshire Safeguarding Children Board procedures.

- The **purpose** of this online safety policy is to:
  - Safeguard and protect all members of Matlock Bath Holy Trinity CofE Primary School community online.
  - Set out key principles expected of all members of the school community at Matlock Bath Holy Trinity CofE Primary School with respect of the use of IT—based technologies. Thus, enabling all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
  - Identify approaches to educate and raise awareness of online safety throughout the community.
  - Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use for the whole school community, including during delivery and participation of remote learning.
  - Identify clear procedures to use when responding to online safety concerns.
  - Minimise the risk of misplaced or malicious allegations made against adults who work with students.

- Matlock Bath Holy Trinity CofE 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
    - Lifestyle websites promoting harmful behaviours
    - Hate content
    - Content Validation: how to check authenticity and accuracy of inline content
  - **Contact:**
    - Being subjected to harmful online interaction with other users
    - Grooming (sexual exploitation, radicalisation, etc)
    - Online bullying in all forms
    - Social or commercial identity theft, including passwords
  - **Conduct:**
    - Personal online behaviour that increases the likelihood of, or causes, harm.
    - Aggressive behaviours
    - Privacy issues, including disclosure of personal information

    - Digital footprint and online reputation
    - Health and wellbeing (amount of time spent online, gambling, etc)
    - Sexting (the sending of sexually explicit photos or messages from a mobile phone)
    - Copyright (little care or consideration for intellectual property and ownership)

1. Policy Scope

- Matlock Bath Holy Trinity CofE Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Matlock Bath Holy Trinity CofE 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.
- Matlock Bath Holy Trinity CofE 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, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as “staff” in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use Policy for staff
- Acceptable Use Policy for children
- Code of Conduct Policy
- Behaviour Policy
- Child Protection Policy
- Confidentiality Reporting Policy
- Curriculum policies, such as: Computing and Relationships, Sex and Health Education (RSHE) Policy
- Data security
- Image use policy
- Mobile phone Policy
- Extremism and Radicalisation Policy
- Blended and Remote Learning policy

2. Monitoring and Review
Next Review Date: February 2022

- Technology in this area evolves and changes rapidly. This school will review this policy at least annually.
  - 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 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, the Headteacher will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding (Nick Whitehead) will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

3. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (**Sally Swain, Headteacher**) has lead responsibility for online safety. ***Whilst activities of the Designated Safeguarding Lead may be delegated to an appropriately trained deputy (Sarah Rouke), overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL***.
- Matlock Bath Holy Trinity CofE Primary School 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/behaviour policy and acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL (Sally Swain) and any deputies (Sarah Rouke) by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

- Ensure parents are directed to online safety advice and information.
- Provide information on the school's website for parents and the community.

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.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, 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 settings safeguarding recording mechanisms.
- Report online safety concerns, as appropriate, to Governing body and other appropriate individuals.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

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 acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery. At Matlock Bath Holy Trinity CofE Primary School, this is done during the autumn term, every academic year; then revisited as necessary in the spring and summer terms.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.

- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Identify students who are involved in cybercrime or those who are technically gifted and talented and are at risk of becoming involved in cybercrime and make a Cyber Choices referral.

Exit Strategy

- At the end of the period of employment to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

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 as directed by the DSL and leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL and deputy DSL 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 and ability) to:

- Engage in age appropriate online safety education opportunities.
- To read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy annually.
- Contribute to the development of online safety policies.
- 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 Pupil Acceptable Use Agreement and encourage their children to adhere to it.

- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from Matlock Bath Holy Trinity CofE Primary School, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately. Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.
- Abide by the home-school agreement and Pupil Acceptable Use Agreement
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in Relationships, Sex and Health Education (RSHE) Policy and computing programmes of study. For examples, see Matlock Bath's RSHE Policy, Safeguarding/British Values Overview and Online Safety Whole School Overview, accessed via our school website: https://www.mbhtprimaryschool.org.uk/policies/
    - 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.
    - Teaching pupils about copyright and data protection. This will be to ensure that pupils are aware of plagiarism, how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.

- The setting will support learners to read and understand the acceptable use policies 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.
    - Implementing appropriate peer education approaches, with older, more experienced children training and supporting other children.
    - 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 online safety policies and practices, including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

- Matlock Bath Holy Trinity CofE Primary School recognises that some learners are 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.
- Matlock Bath Holy Trinity CofE Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners. Needs are met on an individualised basis, and provision and/or intervention will be designed to ensure that each child has full access to the online safety curriculum, with materials and resources that are adapted as necessary to aid understanding and progress.
- When implementing an appropriate online safety policy and curriculum Matlock Bath Holy Trinity CofE Primary School will seek input from specialist staff as appropriate, including the SENCO and other adults that know that child well.

5.3 Training and engagement with staff

We will:

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

5.4 Awareness and engagement with parents and carers

- Matlock Bath Holy Trinity CofE Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats.
        - 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 online safety policy and expectations in newsletters, letters and on our website.
    - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
    - Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- Matlock Bath Holy Trinity CofE 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 the setting is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- Matlock Bath Holy Trinity CofE Primary School uses a wide range of technology. This includes access to:
    - Computers, laptops, iPads and tablets

    - Internet which may include search engines and educational websites
    - Learning platform/intranet (Google Classroom)
    - Email
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our Acceptable Use Policy and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
    - Suggested search engines include Dorling Kindersley Find Out (www.dkfindout.com) , Kiddle, Google Safe Search (https://www.safesearch.com)
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
    - **Early Years Foundation Stage and Key Stage 1**
        - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
    - **Key Stage 2**
        - Learners will use age-appropriate search engines and online tools.
        - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

7.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.
- We will carry our regular audits and audit activity to help identify pupils trying to access sites to establish any vulnerabilities and offer advice, support and react accordingly

7.3 Filtering and Monitoring

7.3.1 Decision Making

- Matlock Bath Holy Trinity CofE Primary School governors and Headteacher (Sally Swain) have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and Headteacher are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- Education broadband connectivity is provided through **KCom Ltd.**
- We use **eSafety4schools** (previously Capital Bytes) which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with **KCom, esafety4schools and Derbyshire School IT Services** to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - **Turn off monitor/screen and report the concern immediately to a member of staff.**
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff, using the form Appendix 1.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Derbyshire Police or CEOP.

7.3.4 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - ***Detail how this will be achieved e.g. physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and/or active/pro-active technology monitoring services.***
- If a concern is identified via monitoring approaches we will:
    - Respond promptly and accordingly in line with the Safeguarding and Child Protection Policy, using Safeguarding Concern Form, the Discussion of Vulnerability form and the Online Safety Incident form (Appendix 1) as appropriate. Escalate this process in the appropriate way.
    - If the concern is in regard to a member of staff's use, respond in line with the Confidential Reporting Code (Whistleblowing Policy).
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection (GDPR), 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 General Data Protection Regulations and Data Protection legislation.

7.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly via School IT.
  - Encryption for personal data sent over the Internet 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 using USB sticks in school.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on our network,
  - The appropriate use of user logins and passwords to access our network.
    - Specific user logins and passwords will be enforced for all but the youngest users.
  - All users are expected to log off or lock their screens/devices if systems are unattended.
  - Further information about technical environment safety and security can be found in pupil AUP, Staff Code of Conduct for IT, the Internet and Electronic Communication, Mobile Phone Policy, GDPR Policy.

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- If using online recording systems, restricted access will be granted per job role and responsibility with regular reviews of who has access
- All learners are provided with their own unique username and private passwords to access our Chromebooks; learners are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system. The longer and more unusual, the stronger the password becomes. Using a combination of upper, lower case, numbers and special characters is recommended.
  - 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.
  - Update password when prompted at pre-planned intervals.

7.6 Managing the Safety of our Website

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

7.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

7.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the 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.
    - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell Sally Swain (Headteacher) if they receive offensive communication, and this will be recorded in our safeguarding files/records.

7.8.1 Staff email

- We have dedicated class email addresses for parents to contact class teachers ash@matlockbath.derbyshire.sch.uk oak@matlockbath.derbyshire.sch.uk willow@matlockbath.derbyshire.sch.uk. These emails have set response times of 8:30am – 4pm.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

- Members of staff will refer to and adhere to and adhere to the Staff Code of Conduct for IT, Internet and Electronic Communication, alongside the Mobile Phone Policy.

7.8.2 Learner email

- Learners will use provided email accounts for educational purposes. These email addresses have no access to emailing services, they are only used for log ins.
- Learners will sign an Acceptable Use for Children Policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the setting.

7.9 Educational use of Videoconferencing and/or Webcams

Matlock Bath Holy Trinity CofE Primary School recognise that videoconferencing and the use of webcams can be a challenging activity but brings a wide range of learning benefits.

  - All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
  - Videoconferencing contact details will not be posted publicly, only within Derbyshire County Council domains.
  - Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
  - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.
  - Pupils are educated about webcams and adhere the Acceptable Use Policy at all times.

7.9.1 Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised by a member of staff at all times.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment, on Google Meets or Teams.
- 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. Staff members can create links to share through Google Classroom or Class Emails.

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, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

7.10 Management of Learning Platforms

- Matlock Bath Holy Trinity CofE Primary School uses Google Classroom as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Children will have individual log ins that they can use to access Google Classroom at school or at home.
- Only current members of staff will have use of Google Classroom.
- When staff and learners leave the setting, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the Google Classroom:
    - Only using their personal log-in and personal password
    - Using standard English (not text speak)
    - If comments are enabled, following clear guidelines to be respectful, positive and specific at all times.
    - Only collaborating on work with adult permission to do so.
    - Only sharing work (within the class) with adult permission to do so.
    - Not uploading content to Google classroom unless instructed to do so.
- All users will be mindful of copyright and will only upload appropriate content onto the Google Classroom.
- Any concerns about content on the Google Classroom 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. Appendix 1 (Online Safety Incident Form) will be used to record this.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to the Google Classroom for the user may be suspended.
    - The user will need to discuss the issues with the headteacher before reinstatement.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures and report to the police.
- 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 Google Classroom by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media and remote learning applies to all members of Matlock Bath Holy Trinity CofE Primary School community.
- Members of staff will refer to and adhere to the school's Staff Code of Conduct for IT, Internet and Electronic Communication and other policies where the staff use of social media is referred to.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site. Access to social media is filtered on school devices. Staff are not permitted to access social media during lesson time or if on duty in other times (e.g. after school club or breakfast time).
- If accessing social media on own devices in own time during the school day, this must not be done in the view of children.
- Matlock Bath Holy Trinity CofE Primary School does not use an official social media channel.
- Concerns regarding the online conduct of any member of Matlock Bath Holy Trinity CofE Primary School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learner's use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities. Staff will seek advice about apps and recommended age limits as part of continuing professional development in online safety Common Sense Media is a useful website to research this.
    - How to block and report unwanted communications.

- How to report concerns both within the setting and externally.

9. Use of Personal Devices and Mobile Phones

- Matlock Bath Holy Trinity CofE 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 the setting.

9.1. Staff Use of Personal Devices and Mobile Phones

- Members of staff will refer to and adhere to the school's acceptable use policy, and Staff Code of Conduct for IT, the Internet and Electronic Communication, alongside any other policy where the staff use of personal devises and mobile phones is referred to.

9.2 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.
- Matlock Bath Holy Trinity CofE Primary School expects learners' personal devices and mobile phones to be handed inn to the office on entry to school. This only takes place after an agreement is signed by the child's parent or carer to allow the device to be carried to and from school. No other devices are permitted in school.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place by the headteacher.
  - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our 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 DfE guidance and our policy. See: www.gov.uk/government/publications/searching-screening-and-confiscation)
  - Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. See: www.gov.uk/government/publications/searching-screening-and-confiscation)
  - 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 learner'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.

9.3 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 our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- We will ensure appropriate signage and information is displayed and 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 DSL (or deputy) of any breaches to our policy.

Responding to Online Safety Incidents and Concerns

- All members of the 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. An Online Safety Incident Form (Appendix 1) will be completed and escalated as required.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
    - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the Confidential Reporting Code (whistleblowing) procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- We will refer to the flow chart on responding to incidents, made available
- Where there is suspicion that illegal activity has taken place, we will follow the local safeguarding procedures which will include Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL, Sally Swain or Deputy DSL, Sarah Rouke will speak with Call Derbyshire/ Derbyshire Police first to ensure that potential investigations are not compromised.
- All members of the community will be made aware of the availability of Cyber Choices or early intervention programmes for individuals who are involved in cybercrime, or those who are gifted and talented and are at risk of becoming involved in cybercrime.

10. Concerns about Learners Welfare

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns via Online Safety Incident Form or Safeguarding Concern Form.
    - The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Derby and Derbyshire Safeguarding Children Partnership thresholds and procedures.

- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

- Our school/ 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.
- Matlock Bath Holy Trinity CofE 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.
- Matlock Bath Holy Trinity CofE 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.
- Matlock Bath Holy Trinity CofE Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Matlock Bath Holy Trinity CofE 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 RSHE 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 Positive 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 our local 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 ("Sexting")

- Matlock Bath Holy Trinity CofE Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We 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".
- Matlock Bath Holy Trinity CofE 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 during PSHE and computing lessons.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We 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.
        - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented on safeguarding concern form.
    - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
    - Act in accordance with our child protection policies and the relevant Derbyshire Safeguarding Child Board's procedures.
    - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Store the device securely.
        - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

    - Carry out a risk assessment which considers any vulnerability of learners 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 Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
    - Implement appropriate sanctions in accordance with our 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 DSL 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.

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

- Matlock Bath Holy Trinity CofE 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.
- Matlock Bath Holy Trinity CofE 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. https://www.mbhtprimaryschool.org.uk/useful-links/
- 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 our local 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 Derbyshire police by using 101.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Derbyshire police using 101 unless immediate concerns and 999 will be used 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 first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- Matlock Bath Holy Trinity CofE Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek 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 we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire Police using 101.

- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy and the relevant Derby City & Derbyshire Safeguarding Child Boards procedures.
    - 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 learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy) 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 setting provided devices, we will:
    - Ensure that the DSL (or deputy) 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 Derbyshire police via 101 (999 if there is an immediate risk of harm) and Children's Services using Call Derbyshire (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.
    - 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 setting provided devices, we will:
    - Ensure that the headteacher, Sally Swain, is informed immediately and without any delay in line with our Managing Allegations against Staff policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our Managing Allegations against Staff policy.
    - Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Matlock Bath Holy Trinity CofE Primary School.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy. See policy at: https://www.mbhtprimaryschool.org.uk/policies/

11.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Matlock Bath Holy Trinity CofE Primary School and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.

- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Derbyshire police and or the safer Derbyshire website https://www.saferderbyshire.gov.uk/home.aspx

11.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. For more detail, revisit Section 7. We have adopted the Derbyshire Extremism and Radicalisation Policy 2017.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy and Derbyshire prevent pathway which may include a referral into Channel.
- If we are concerned that member of staff may be at risk of radicalisation online, the headteacher, Sally Swain, will be informed immediately, and action will be taken in line with the Child Protection Policy and Confidential Reporting Code (whistleblowing policy).

11.8 Cybercrime

Cybercrime incidents and offences will be responded to in line with our existing behaviour policies.

We will respond to concerns that our students are involved, or at risk of becoming involved, in cybercrime, even if it takes place off site.

We will make a Cyber Choices referral for early intervention, as per the Cyber Choices Toolkit.

If we are concerned that a child is being exploited as a result of their technical skills, we will follow the Children at Rick of Exploitation (CRE) procedure and the CRE Risk Assessment Toolkit.

12. Useful Links for Educational Settings

Support and Guidance for Educational Settings

Derby City & Derbyshire Safeguarding Children Board online procedures DSCB:

- **http://derbyshirescbs.proceduresonline.com/**

Derbyshire Police:

- 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

LADO

- By referral into Professional.Allegations@derbyshire.gov.uk
- Form found here http://derbyshirescbs.proceduresonline.com/docs_library.html

Call Derbyshire (Starting Point)

- Immediate risk of harm phone 01629 533190
- For all other referrals complete an online form https://www.derbyshire.gov.uk/social-health/children-and-families/support-for-families/starting-point-referral-form/starting-point-request-for-support-form.aspx
- For professional advice phone 10629 535353

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Child net: www.childnet.com
- 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
- Child net: 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

Signed by:

Chair of Governors	Headteacher
Date:	Date: