

Boughton-under-Blean & Dunkirk Methodist School Online Safety Policy



Key Details

Designated Safeguarding Lead: Jo Cottenden

Named Governor with lead responsibility: Michael Baybutt

Date written: October 2022

Date agreed and ratified by Governing Body: 26/9/22

Date of next review: October 2023

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.

Doing all the good that we can

We aspire for all our children to become confident, happy and caring individuals who achieve personal success and develop a love of learning and a life built upon our school values.

Boughton-under-Blean & Dunkirk is a Methodist Primary School and our Methodist values are at the heart of everything we do.

- Forgiveness
- Friendship
- Trust
- Justice
- Perseverance

These are then underpinned by our learning values.

- Communication
- Independence
- Aspiration
- Engagement

Our whole school ethos is built upon and guided by them. Every school policy is written with this in mind and implemented in way that reflects our vision of doing all the good that we can and developing children as life long learners.

'Start children off on the way they should go, and even when they are old they will not turn from it'

Proverbs 22:6

Boughton-under-Blean & Dunkirk Methodist Primary School Online Safety Policy

1. Policy Aims and Scope

- This online safety policy has been written by Boughton-under-Blean & Dunkirk Methodist Primary School, involving staff, pupils and parents/carers, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance '[Keeping Children Safe in Education](#)' 2022, '[Early Years and Foundation Stage](#) 2017, '[Working Together to Safeguard Children](#)' 2018 and the local [Kent Safeguarding Children Multi-agency Partnership](#) (KSCMP) procedures.
- The purpose of Boughton-under-Blean & Dunkirk Methodist Primary School's online safety policy is to:
 - Safeguard and protect all members of Boughton-under-Blean & Dunkirk Methodist Primary School 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.
- Boughton-under-Blean & Dunkirk Methodist 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
 - **Contact:** being subjected to harmful online interaction with other users
 - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
- Boughton-under-Blean & Dunkirk Methodist Primary School believes that online safety is an essential part of safeguarding and acknowledges it's duty to ensure that all pupils and staff are protected from potential harm online.
- Boughton-under-Blean & Dunkirk Methodist 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 which present positive and exciting opportunities, as well as challenges and risks.
- Boughton-under-Blean & Dunkirk Methodist Primary School believes that pupils 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 using the school's network, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.
- 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
 - Behaviour and discipline policy
 - Child protection policy

- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
- Data security
- Image use policy
- Searching, screening and confiscation policy

2. Responding to Emerging Risks

Boughton-under-Blean & Dunkirk Methodist 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:

- carry out an annual review of our online safety approaches which will be supported by an annual risk assessment which considers and reflects the specific risks our learners face.
- regularly review the methods used to identify, assess and minimise online risks.
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use is permitted.
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that internet access is appropriate.
- recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems, and as such identify clear procedures to follow if breaches or concerns arise.

3. Monitoring and Review

- Boughton-under-Blean & Dunkirk Methodist Primary School will review this policy at least annually. The policy will also be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems 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.
- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.
- Any issues identified will be incorporated into our action planning.

4. Roles and Responsibilities

- The school has appointed Mrs Jo Cottenden, as Designated Safeguarding Lead to be the online safety lead.
- Boughton-under-Blean & Dunkirk Methodist 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:

- Create a whole setting culture that incorporates online safety throughout all elements of school life.

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with technical staff and IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

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 such as pastoral support staff, IT technicians, network managers and the SENCO as appropriate.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside other DSLs in the school to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated whole school approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge 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.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- 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 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 senior leadership 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 regularly (twice yearly) with the governor with a lead responsibility for safeguarding and/or 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 AUPs..
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology.
- Maintain a professional level of conduct in their personal use of technology, both on and off site as stated in the Acceptable Use Policy.
- 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.

4.5 It is the responsibility of pupils (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. Appropriate training for parents may be given from time to time.
- Encourage 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 through parent governors where appropriate.
- Use school 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.

5. Education and Engagement Approaches

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 our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) '[Education for a Connected World Framework](#)' and DfE '[Teaching online safety in school](#)' guidance.
 - ensuring education regarding safe and responsible use precedes internet access.
 - ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study.
 - reinforcing online safety messages whenever technology or the internet is in use.
 - creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
 - involving the DSL (or a deputy) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content.
 - making informed decisions to ensure that any educational resources used are appropriate for our learners.
 - using external visitors, where appropriate, to complement and support our internal online safety education approaches.
 - providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
 - rewarding positive use of technology.
- The school will support pupils 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.
 - seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- Boughton-under-Blean & Dunkirk Methodist Primary School will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
 - ensuring age appropriate education regarding safe and responsible use precedes internet access.
 - teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
 - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
 - enabling them to understand what acceptable and unacceptable online behaviour looks like.
 - preparing them to identify possible online risks and make informed decisions about how to act and respond.
 - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Pupils

- Boughton-under-Blean & Dunkirk Methodist Primary School recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- Boughton-under-Blean & Dunkirk Methodist Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- Boughton-under-Blean & Dunkirk Methodist Primary School will seek input from specialist staff as appropriate, including the SENCO (Mrs Kay Lewis) and Family Liaison Officer (Laura Jakob).

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

5.4 Awareness and engagement with parents and carers

- Boughton-under-Blean & Dunkirk Methodist 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.

6. Reducing Online Risks

- Boughton-under-Blean & Dunkirk Methodist 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

- Boughton-under-Blean & Dunkirk Methodist Primary School uses a wide range of technology. This includes access to:
 - Computers, laptops and other digital devices
 - Internet which may include search engines and educational websites
 - School learning platform/intranet
 - Email
 - 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.
- 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 Safesearch, Dorling Kindersley Find Out, 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**
 - Pupils' 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 pupils' age and ability.
 - **Key Stage 2**
 - Pupils will use age-appropriate search engines and online tools.
 - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

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, pupils 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

- Boughton-under-Blean & Dunkirk Methodist Primary School's 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. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
- 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 EiS.
- The school uses EiS (Lightspeed) which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. YouTube is permitted to be used by teaching staff as a teaching tool but this is blocked for use by pupils.
 - The school filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.

- It integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'
- The school works with EiS 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 press the back button or turn off the screen and 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, Kent 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:
 - physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and/or active/pro-active technology monitoring services.
- The school has a clear procedure for responding to concerns identified via monitoring approaches. The DSL will respond in line with the child protection policy.
- 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.
- If a concern is identified via our monitoring approaches:
 - Where the concern relates to learners, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour.
 - Where the concern relates to staff, it will be reported to the headteacher (or chair of governors if the concern relates to the headteacher), in line with our staff behavior and allegations policy.

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.
 - Full information can be found in the school's 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.

- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
- Checking files held on our network, as required and when deemed necessary by leadership staff.
- The appropriate use of user logins and passwords to access our network. Specific user logins and passwords will be enforced for all users.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- We will review the effectiveness of our security approaches and procedures periodically in order to keep up with evolving cyber-crime technologies.

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 5, all pupils are provided with their own unique username and private passwords to access school systems; pupils are responsible for keeping their password private.
- We require all users to:
 - Use strong passwords for access into our system.
 - Change their passwords every 6 months.
 - 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.
 - Lock access to devices/systems when not in use.

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 pupils' 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 policies, 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.

- 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 Mr Simon Way (Headteacher) 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.

7.8.1 Staff

- 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 Pupils

- Pupils will use school provided email accounts for educational purposes.
- Pupils will sign an AUP 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 school.

7.9 Educational use of Videoconferencing and/or Webcams

- Boughton-under-Blean & Dunkirk Methodist Primary School recognise that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits. Staff will refer to the Remote Learning AUP.
 - All videoconferencing 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.
 - Video conferencing 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.
 - Videoconferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Parents and carers' consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils 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.
- 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.

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.

7.10 Management of Learning Platforms

- Boughton-under-Blean & Dunkirk Methodist Primary School uses DB Primary, Google Classroom and Purple Mash as its official learning platforms.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff, pupils 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. e) A pupil's 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.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil 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 does not use any application to track pupils' progress.
- 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.
- In order to safeguard pupils data:
 - 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 Management of remote learning

Where children are asked to learn online at home in response to a full or partial closure:

- Boughton-under-Blean & Dunkirk Methodist Primary School will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.
- All communication with learners and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and agreed systems e.g. Google Classroom.
 - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.
- Staff and learners will engage with remote teaching and learning in line with existing behaviour principles as set out in our Acceptable Use Policies.
- Staff and learners will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.
- When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP)
- Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. Boughton-under-Blean & Dunkirk Methodist Primary School will continue to be clear who from the school their child is going to be interacting with online.
- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

9. 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.
 - Pupils, 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 pupils 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 Kent 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 Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about learner online behaviour and/or 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 Kent Safeguarding Children Board thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2 Concerns about staff online behaviour and/or welfare

- 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.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the headteacher and/or DSL (or deputy). The headteacher and/or DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, acceptable use of technology and behaviour policy.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

11. Procedures for Responding to Specific Online Incidents or Concerns

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) and part 5 of '[Keeping children safe in education](#)' 2020.
 - Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.
- Boughton-under-Blean & Dunkirk Methodist 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

- 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
- Unwanted sexual comments and messages on social media
- Online sexual exploitation
- 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 Kent 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.
- Boughton-under-Blean & Dunkirk Methodist Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, the 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 by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

11.2 Youth Produced Sexual Imagery ("Sexting")

- Boughton-under-Blean & Dunkirk Methodist 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 UKCIS guidance: ['Sexting in schools and colleges: responding to incidents and safeguarding young people'](#) and [KSCB](#) guidance: "Responding to youth produced sexual imagery".
 - Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
 - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.

- Boughton-under-Blean & Dunkirk Methodist 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.
- 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.
 - 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 Kent 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 UKCIS : ['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 UKCIS: ['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)

- Boughton-under-Blean & Dunkirk Methodist Primary School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our child protection policy.

- Boughton-under-Blean & Dunkirk Methodist 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.
- 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 can be found on our school website homepage.
- 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 Kent 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 Kent 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 Kent 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 Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- Boughton-under-Blean & Dunkirk Methodist 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 Kent Police and/or the Education Safeguarding Team.
- If made aware of IIOC, we will:
 - Act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent 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 police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (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 setting provided devices, we will:
 - Ensure that the Headteacher is informed 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 Boughton-under-Blean & Dunkirk Methodist Primary School

- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

11.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Boughton-under-Blean & Dunkirk Methodist 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 Education Safeguarding Team and/or Kent Police.

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.
- 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.
- If we are 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 Cybercrime

- Boughton-under-Blean & Dunkirk Methodist Primary School recognises that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer/internet enabled device) cybercrime.
- If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL will be informed, and consideration will be given to accessing local support and/or referring into the [Cyber Choices](#) programme, which aims to intervene when young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

12. Useful Links

Links for Schools

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
- SWGfL: 360 Safe Self-Review tool for schools www.360safe.org.uk
- Childnet: www.childnet.com
 - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
 - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools
- PSHE Association: www.pshe-association.org.uk
- National Education Network (NEN): www.nen.gov.uk
- National Cyber Security Centre (NCSC): www.ncsc.gov.uk
- Educate against hate: <https://educateagainsthate.com>
- NCA-CEOP Education Resources: www.thinkuknow.co.uk
- Safer Recruitment Consortium: www.saferrecruitmentconsortium.org/

Reporting Helplines

- NCA-CEOP Safety Centre: www.ceop.police.uk/Safety-Centre
- Internet Watch Foundation (IWF): www.iwf.org.uk
- ChildLine: www.childline.org.uk
 - Report Remove Tool for nude images: [www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online](http://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety sexting/report-nude-image-online)
- Stop it now! www.stopitnow.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Report Harmful Content: <https://reportharmfulcontent.com>
- Revenge Porn Helpline: <https://revengepornhelpline.org.uk>
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Support for children and parents/carers

- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Parent Zone: <https://parentzone.org.uk>
- NSPCC: www.nspcc.org.uk/onlinesafety
 - Net Aware: www.net-aware.org.uk
- Parents Protect: www.parentsprotect.co.uk
- Get Safe Online: www.getsafeonline.org
- NCA-CEOP Child and Parent Resources: www.thinkuknow.co.uk