Blean Primary School
Online Safety Policy

Key Details

Designated Safeguarding Lead (s): Ian Rowden, Kara Satterley, Nicki Llewellyn, Lynda Prior, Lorraine Watson and Jane Williams

Named Governor with lead responsibility:

Hugh Samuelson

Date updated: October 2024

Date agreed and ratified by Governing Body:

Date of next review: October 2025

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.

Blean Primary School Online Safety Policy

Contents

Blean Primary School .....

Policy Aims and Scope 3

1. Responding to Emerging Risks 4

2. Monitoring and Review 4

3. Roles and Responsibilities 4

4. Education and Engagement Approaches 7

5. Safer Use of Technology 9

6. Cyber-bullying 15

7. Social Media 17

8. Use of Personal Devices and Mobile Phones 20

9. Responding to Online Safety Incidents and Concerns 22

10. Procedures for Responding to Specific Online Incidents or Concerns 23

Useful Links 31

Policy Aims and Scope

- This online safety policy has been written by Blean Primary School, involving staff and pupils and consultation with parents/carers, building on The Education People online safety policy template, with specialist advice and input 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 local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.
- We recognise that online safety is an essential part of safeguarding and acknowledge our duty to ensure that all learners and staff are protected from potential harmful and inappropriate online material and/or behaviour. This policy sets out our whole school approach to online safety which will empower, protect and educate learners and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.
- understands that breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
    - **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
    - **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
    - **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
    - **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
- Blean Primary recognises that children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online
- Blean 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.
- 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 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 mobile technology, or where pupils, staff or other individuals have been provided with school issued devices for use both on and off-site, such as a work laptop, tablet or mobile phone.
- This policy links with a number of other policies, practices and action plans including:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and our Code of conduct
    - Behaviour policy
    - Child protection policy
    - Confidentiality policy
    - Curriculum schemes, such as: Computing, Personal Social and Health Education (PSHE), Relationships Education (RSE)
    - Data security

- Image use policy
- Searching, screening and confiscation (DFE Guidance)
- Social Media Policy
- Mobile and Smart Technology Policy

1. Responding to Emerging Risks

- Blean Primary 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.
  - regularly review the methods used to identify, assess and minimise online risks.
  - examine emerging technologies for educational benefit 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.

2. Monitoring and Review

- Blean Primary 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, as appropriate.
- 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.

3. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Mr Ian Rowden is recognised as holding overall lead responsibility for online safety.
- Blean Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

3.1 The leadership team will:

- Create a whole setting culture that incorporates online safety throughout all elements of Blean Primary 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.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of conduct and an AUP, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Support the Designated Safeguarding Lead and deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, pupils 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.

3.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues.
- Liaise with other members of staff, such as the Parent-Pupil Mentor, IT technician and Inclusion Manager on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole Blean Primary 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.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day (SID).
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

- Meet regularly with the Computing lead Ashley Hoskins and the governor with a lead responsibility for safeguarding and/or online safety.

3.3 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 of technology policies.
- Take responsibility for the security of school IT systems and the electronic data they use or have access to.
- Model good practice when using technology with pupils.
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting pupils and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

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

- Provide technical support and perspective to the DSL and the school's 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 our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action when required.

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

- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the school acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others both on and offline.
- Take an appropriate level of 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.

3.6 It is the responsibility of parents and carers to:

- Read the school acceptable use of technology policies and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and acceptable use of technology policies. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies.
- Use the 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.

4. Education and Engagement Approaches

4.1 Education and engagement with pupils

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in the PSHE, SRE and Computing programmes of study, covering use both at home school and home Reinforcing online safety messages whenever technology or the internet is in use.
    - Implementing appropriate peer education approaches.
    - 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.
    - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - 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.
    - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
    - 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.
- Blean Primary School will support pupils to understand and follow 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 pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Implementing appropriate peer education approaches through the e-safety ambassador team.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.

- Blean 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.

4.2 Vulnerable Pupils

- Blean Primary School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Blean Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to all learners who require additional or targeted support.
- Blean Primary School will seek input from specialist staff as appropriate, including the DSL, Inclusion Manager and Extended Schools Manager to ensure that the policy and curriculum is appropriate to our community's needs.

4.3 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 via our child protection training, email and staff learning sessions to follow up any e-safety concerns as they occur.
    - 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.

4.4 Awareness and engagement with parents and carers

- Blean 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 and Safer Internet Day (SID) activities.
    - Drawing their attention to the school online safety policy and expectations in newsletters, letters 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 acceptable use policies and discuss its implications with their children.

5. Safer Use of Technology

5.1 Classroom Use

- Blean 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
    - Games consoles and other games based technologies
    - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's acceptable use policy and with appropriate safety and security measures in place. Mobile device management software Meraki is used.
- 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 in line with SNS recommendations.
- 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.

5.2 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 acceptable use policy before being given access to the school computer system, IT resources or internet.

5.3 Filtering and Monitoring

5.3.1 Decision Making

- Blean School will do all we reasonably can to limit children's exposure to online risks through school provided IT systems/devices and will ensure that appropriate filtering and monitoring systems are in place.
- Blean School governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.
- Blean Primary School governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- 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.

5.3.2 Appropriate Filtering

- Blean School uses educational broadband connectivity through (Kent School Broadband)
- Blean School uses (Light-speed Filtering System) which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
    - The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list and blocks access to illegal Child Abuse Images and Content (CAIC).
- Blean School works with (Kent School Broadband) to ensure that our filtering policy is continually reviewed.

5.3.3 Dealing with Filtering breaches

- Blean School has a clear procedure for reporting filtering breaches.
    - If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediate 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.

5.3.4 Appropriate Monitoring

- Blean School will appropriately monitor internet use on all school owned or provided internet-enabled devices. This is achieved by: Close supervision of pupils, monitoring internet and web access information by random checks by IT Technician with log kept by Schools Business Manager.
- 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

5.4 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.

5.5 Information Security and Access management

- 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 the school network.
        - Specific user logins and passwords will be enforced for all.
    - 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 our School AUPs wifi use agreement and online safety concerns flowchart.

- We will review the effectiveness of our security approaches and procedures periodically in order to keep up with evolving cyber-crime technologies.

5.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.
- From year *3*, all 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 term.
    - 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.

5.6 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.

5.7 Publishing Images and Videos Online

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

5.8 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. (KLZ to KLZ or password protected)
- 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 a member of SLT if they receive offensive communication, and this will be recorded in the school safeguarding files/records.

- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school.

5.8.1 Staff email

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

5.8.2 Pupils email

- Pupils will use school provided email accounts for educational purposes.
- Pupils will agree an acceptable use 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 school

5.9 Educational use of Videoconferencing and/or Webcams

- Blean Primary School recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites. (Kent School Broadband)
    - Videoconferencing contact details will not be posted publically.
    - School videoconferencing equipment will not be taken off school premises without prior permission from the DSL.
    - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

5.9.1 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 with a member of Blean Staff present at all times.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment e.g. through Microsoft 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.

5.9.2 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.

5.10 Management of Learning Platforms

- Blean Primary School uses Google Classroom as its official learning platform.
- 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.

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

- The school uses Tapestry to track pupils progress and share appropriate information with parents and carers.
- The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and 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.

5.12 Management of remote learning

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

- Blean Primary 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 or other agreed systems e.g. Google Classroom, Microsoft 365 or equivalent.
    - 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 behaviour policy/code of conduct and 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. Blean Primary 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.

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.4 Artificial intelligence (AI)

- Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.
- Blean Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.
- Blean Primary School will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.
- Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

7. Social Media

7.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Blean Primary School community. The policy applies to all use of social media; the term social media includes, but is not limited to, blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger apps or other online communication services.

- All members of Blean Primary School community are expected to engage in social media in a positive, safe and responsible manner, at all times.
- All members of Blean Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

- The school will control pupil and staff access to social media whilst using school provided devices and systems on site. (Kent School Broadband will block all social media sites i.e: Facebook, snapchat etc)
- The use of social media during school hours for personal use **by pupils is not** permitted.
- Staff access via 4/4G is only acceptable during breaks, lunch and away from children.
- Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Blean 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.

7.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the AUP.
- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

7.2.1 Reputation

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

- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

7.2.2 Communicating with pupils and parents and carers

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

7.3 Pupils' Personal Use of Social Media

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

8. Use of Personal Devices and Mobile Phones

- Blean Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

8.1 Expectations

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

8.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child protection, Data security and Acceptable use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time locked in a drawer or cupboard.
    - Keep mobile phones and personal devices switched off or switched to ‘silent’ mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as ‘airdrop’) are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless written permission has been given by the Headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead/Headteacher.

- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
    - Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the school Disciplinary and Allegations policy
    - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

8.3 Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Blean Primary School expects pupils' personal devices and mobile phones to be switched off handed in and stored securely by Class Teacher during the school day.
- If a pupil needs to contact his/her parents or carers they will be allowed to use a **school phone.**
    - Parents are advised to contact their child via the school office during school hours; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time.
- Mobile phones and personal devices must not be taken into examinations such as SATS or Kent Test.
    - Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place.
    - School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting).
    - Searches of mobile phone or personal devices will only be carried out in accordance with the DFE guidance. www.gov.uk/government/publications/searching-screening-and-confiscation)
    - Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes school policies.
    - Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the school day.
    - If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

8.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Child protection and Image use.
- The school will ensure appropriate signage and information is displayed to inform parents, carers and visitors of expectations of use.

- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

8.5 Officially provided mobile phones and devices

- Members of staff may be issued with a work phone number and email address, where contact with pupils or parents/ carers is required.
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the Acceptable use policy, Code of Conduct and Staff Handbook.

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 (or deputy) 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 DSL will speak with Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

9.1 Concerns about Pupils 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.

9.2 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 Disciplinary policy and Code of conduct.
- Welfare support will be offered to staff as appropriate.

9.3 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, home-school agreements, 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

10. Procedures for Responding to Specific Online Incidents or Concerns

10.1 Online child on child abuse

- Blean Primary recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online child on child abuse concerns will be responded to in line with our child protection and behaviour policies.
- We recognise that online child on child abuse can take many forms, including but not limited to:
  - bullying, including cyberbullying, prejudice-based and discriminatory bullying
  - abuse in intimate personal relationships between peers
  - physical abuse, this may include an online element which facilitates, threatens and/or encourages physical abuse
  - sexual violence and sexual harassment, which may include an online element which facilitates, threatens and/or encourages sexual violence
  - consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)
  - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
  - upskirting (which is a criminal offence), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
  - initiation/hazing type violence and rituals.
- Blean Primary believes that abuse is abuse, including when it takes place online and it will never be tolerated or dismissed as "banter", "just having a laugh", "part of growing up" or "boys being boys" as this can lead to a culture of unacceptable behaviours and an unsafe environment for children.
- Blean Primary believes that all staff have a role to play in challenging inappropriate online behaviours between peers.
- Blean Primary recognises that, even if there are no reported cases of online child on child abuse, such abuse is still likely to be taking place.
- Concerns about learner's behaviour, including child on child abuse taking place online offsite will be responded to as part of a partnership approach with learners and parents/carers and in line with existing policies, for example anti-bullying, acceptable use, behaviour and child protection policies.

- Blean Primary want children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online child on child abuse will be reported to the DSL and will be recorded, investigated, and dealt with in line with associated policies, including child protection, anti-bullying and behaviour. Learners who experience abuse will be offered appropriate support, regardless of where the abuse takes place

10.1.1 Child on child online sexual violence and sexual harassment

- When responding to concerns relating to online child on child sexual violence or harassment, Blean Primay will follow the guidance outlined in Part Five of KCSIE 2021 and the DfE 'Sexual Violence and Sexual Harassment Between Children in Schools and Colleges' guidance.
- Online sexual violence and sexual harassment exists on a continuum and may overlap with offline behaviours; it is never acceptable. Abuse that occurs online will not be downplayed and will be treated equally seriously.
- All victims of online sexual violence or sexual harassment will be reassured that they are being taken seriously and that they will be supported and kept safe. A victim will never be given the impression that they are creating a problem by reporting online sexual violence or sexual harassment or be made to feel ashamed for making a report.
- Blean Primary recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - consensual and non-consensual sharing of nude and semi-nude images and videos
    - sharing of unwanted explicit content
    - 'upskirting' (which is a criminal offence and typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm)
    - sexualised online bullying
    - unwanted sexual comments and messages, including, on social media
    - sexual exploitation, coercion and threats.
- Blean Primary recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection to face to face incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and 24 services, and for things to move from platform to platform online.
- Blean Primary 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.
- Blean Primary 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 and the support available, by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- When there has been a report of online sexual violence or harassment, the DSL will make an immediate risk and needs assessment which will be considered on a case-by-case basis which explores how best to support and protect the victim and the alleged perpetrator and any other children involved/impacted.
    - The risk and needs assessment will be recorded and kept under review and will consider the victim (especially their protection and support), the alleged perpetrator, and all other children and staff and any actions that are required to protect them.
    - Reports will initially be managed internally by the DSL, and where necessary will be referred to Children's Social Care and/or the Police.

- The decision making and required action taken will vary on a case by case basis but will be informed by the wishes of the victim, the nature of the alleged incident (including whether a crime may have been committed), the ages and developmental stages of the children involved, any power imbalance, if the alleged incident is a one-off or a sustained pattern of abuse, if there are any ongoing risks to the victim, other children, or staff, and any other related issues or wider context.
- If content is contained on learners' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

- Following an immediate risk assessment the school will:
  - provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
  - inform parents/carers for all children involved about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
  - if the concern involves children and young people at a different educational school, the DSL will 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 will discuss this with the 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.
- Blean Primary recognises that internet brings the potential for the impact of any concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. The school also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

10.1.2 Nude or semi-nude image sharing by children

The term 'sharing nudes and semi-nudes' is used to mean the sending or posting of nude or semi-nude images, videos or live streams of/by young people under the age of 18. Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents complex. The UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance outlines how schools and colleges should respond to all incidents of consensual and non-consensual image sharing, and should be read and understood by DSLs working will all age groups.

- Blean Primary recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") can be a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- This policy defines sharing nude or semi-nude image sharing as when a person under the age of 18:
  - creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.
  - shares nude and/or semi-nude imagery created by another person under the age of 18 with a peer(s) under the age of 18.
  - possesses nude and/or semi-nude imagery created by another person under the age of 18.

- When made aware of concerns regarding nude and/or semi-nude imagery, Blean Primary will follow the advice as set out in the non-statutory UKCIS guidance: 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- Blean Primary will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing nude or semi-nude images and sources of support, by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will respond to concerns regarding nude or semi-nude image sharing, regardless of whether the incident took place on site or using school provided or personal equipment.
- When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:
    - Report any concerns to the DSL immediately.
    - Never view, copy, print, share, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery by accident, this will be immediately reported to the DSL.
    - Not delete the imagery or ask the child to delete it.
    - Not say or do anything to blame or shame any children involved.
    - Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
    - Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.
- If made aware of an incident involving nude or semi-nude imagery, DSLs will:
    - act in accordance with our child protection policies and the relevant local procedures and in line with the UKCIS guidance.
    - carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
    - a referral will be made to Children's Social Care and/or the police immediately if:
        - the incident involves an adult (over 18).
        - there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
        - the image/videos involve sexual acts and a child under the age of 13, depict sexual acts which are unusual for the child's developmental stage, or are violent.
        - a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.
    - The DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.
    - If DSLs are unsure how to proceed, advice will be sought from the local authority.
    - Store any devices securely:
        - If content is contained on learners' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If a potentially 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.

- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
- provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- implement sanctions where necessary and appropriate 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 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.
    - Learners will be supported in accessing the Childline 'Report Remove' tool where necessary: Report Remove Tool for nude images.
- 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.

- We will not:
    - view any imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so. If it is deemed necessary, the imagery will only be viewed where possible by the DSL in line with the national UKCIS guidance, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video of a child and will not allow or request learners to do so.

10.1.3 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Blean Primary.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

10.2 Online child abuse and exploitation

- Blean 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.
- Blean Primary School will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community.
- If the school are made aware of incident involving online sexual abuse of a child, the school will:

    - Act in accordance with the school's Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
    - Immediately notify the Designated Safeguarding Lead.

    - Store any devices involved securely.
    - 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 pupil(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - Make a referral to Children's Social Work Service (if required/ appropriate).
    - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
    - Where possible pupils 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 the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school is 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 Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

10.3 Indecent Images of Children (IIOC)

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

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

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

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

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

10.4 Online hate

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

10.5 Online radicalisation and extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection policy.

- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies.

10.6 Cybercrime

- Blean Primary 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.

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
- 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.ukGet Safe Online: www.getsafeonline.org
- NCA-CEOP Child and Parent Resources: www.thinkuknow.co.uk