Online Safety Policy

Including Use of Social Media and Mobile Technology

BOROUGH GREEN
Primary School

'Learning Together with Kind Hearts and Determined Minds'

Designated Safeguarding Lead: Stella Martin

Deputy DSL: Gretchen Hemsley, Joe Wheatley

Named Governor/s with lead responsibility:

Julie Harvey and Claire Nash

Date written: September 2022

Updated: November 2023

Date agreed and ratified by Governing Body: 30th November 2023

Date of next review: November 2024

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

Borough Green Primary School Online Safety Policy

1. Policy aims

- This online safety policy has been written by Borough Green Primary School, building on the Kent County Council/The Education People online safety policy template, with specialist adviceand 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 andthe local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.

- The purpose of Borough Green Primary School's online safety policy is to
    - safeguard and promote the welfare of all members of Borough Green Primary School community online.
    - identify approaches to educate and raise awareness of online safety throughout our 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 follow when responding to online safety concerns.

- Borough Green 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.
    - **Commerce**: risks such as online gambling, inappropriate advertising, phising and or financial scams.

2. Policy scope

- Borough Green Primary School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Borough Green 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.
- Borough Green Primary School will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online 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 Borough Green Primary School (collectively referred to as “staff” in this policy) as well as learners and parents and carers.

- This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting-issued devices for use, both on and off-site.

2.2 Links with other policies and practices

- This policy links with several other policies, practices and action plans, including but not limited to:
    - Acceptable Use Policy
    - Behaviour Policy
    - Child protection Policy
    - Curriculum Policies, such as the RSE policy
    - Data Protection and GDPR policy

3. Monitoring and review

- Technology evolves and changes rapidly; as such Borough Green Primary School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on online safety practice and incidents,including outcomes, on a regular basis to the wider Governing Body.
- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) and Headteacher are recognised as holding overall lead responsibility for online safety.
- Borough Green 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, child on child 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 that all children at Borough Green Primary School know who to talk to if they are concerned about online content.
- Ensure that staff are aware of the additional risks online to SEND and vulnerable children.
- 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 as well as being taught discreetly in the PHSE, RSHE and Computing curriculums.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with other members of staff, such as IT technicians and the 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 school's 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 school's safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends and use this data to update the education response and school policies and procedures.
- Report online safety concerns, as appropriate, to the school leadership team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis(at least annually).
- Meet each seasonal term with the governor with a lead responsibility for safeguarding.

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

- Contribute to the development of our online safety policies.
- Read and adhere to our online safety policy and acceptable use of technology policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with learners
- Maintain a professional level of conduct in their personal use of technology, both on and offsite.
- 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 learners in their care.
- Identify online safety concerns and take appropriate action by following the school safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting learners and parents/carers 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 school leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures including locking of computers when staff are not in the classroom as directed by the leadership team to ensure that the settings IT infrastructure 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.

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

- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything they or others experience online.

4.6 It is the responsibility of parents and carers to:

- Read our acceptable use of technology policies and encourage their children to adhere tothem.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Seek help and support from Borough Green Primary School or other appropriate agencies if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as learning platforms and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

5. Education and engagement approaches

5.1 Education and engagement with learners

- The setting will establish and embed a whole school culture and will raise awareness andpromote safe and responsible internet use amongst learners by:
    - ensuring our curriculum and whole school approach is developed in line with the UKCouncil for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance.
    - ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study.
    - reinforcing online safety principles in other curriculum subjects as appropriate, andwhenever technology or the internet is used on site.
    - 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.
- being aware that children may not feel ready or know how to tell someone they are being abused; this is especially likely to be the case where abuse takes place online.

- Borough Green Primary School will support learners to understand and follow our acceptable use policies in a way which suits their age and ability by:
  - displaying acceptable use posters in all rooms with internet access.
  - informing learners that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
  - seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- Borough Green 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 Learners

- Borough Green 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.

- Borough Green Primary School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.

- Staff at Borough Green Primary School will seek input from specialist staff as appropriate,including the DSL and Inclusion Manager, to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 Training and engagement with staff

- We will
    - provide and discuss the online safety policy and procedures with all members of staff as part of induction.
    - provide up-to-date and appropriate online safety training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach.
    - staff training covers the potential risks posed to learners (content, contact, conduct and commerce) as well as our professional practice expectations.
    - build on existing expertise by providing opportunities for staff to contribute to and shape our online safety approaches, including curriculum, policies and procedures.
    - make staff aware that our IT systems are monitored, and that activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
    - make staff aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.
    - highlight useful educational resources and tools which staff could use with learners.
    - ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community.
    - ensure staff are aware of how to respond appropriately to incidents involving harmful online challenges and online hoaxes.
    - ensure staff are aware of the 4 c's of the online safety curriculum: Content; Contact; Conduct; Commerce.
    - Training for governors and trustees will focus on the governor's strategic role and responsibility regarding online safety and will ensure they can support the delivery of a robust whole school approach to online safety.

5.4 Awareness and engagement with parents and carers

- Borough Green Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - providing information and guidance on online safety in a variety of formats.
    - providing more specific but proportional information and guidance to parents

should an online hoax or harmful online challenge be affecting our pupils.
    - drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters) as well as in our prospectus and on our website.
    - requesting parents and carers read online safety information as part of joining our community, for example, within our home school agreement.

6. Reducing Online Risks

- Borough Green 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 therefore:

- 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 in the school is permitted.
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that 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 or devices and as such identify clear procedures to follow if breaches or concerns arise.
- Ensure that all members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence. This is clearly outlined in our acceptable use of technology policies and highlighted through a variety of education and training approaches.
- Make staff aware that technology is a significant component in many safeguarding and wellbeing issues.
- Make staff aware that children can abuse other children online. (See Section 11 below)
- Make staff aware that learners frequently acknowledge that they are unlikely to report concerning online behaviours if they are using what adults consider to be 'inappropriate' social media platforms or gaming sites. When children disclose exposure to such sites and games, it will be reported to the DSL or deputy as a safeguarding concern.
- Ensure that staff will provide safe and open spaces for children to ask questions and share concerns without being made to feel foolish or blamed.

7. Safer Use of Technology

7.1 Classroom use

- Borough Green Primary School uses a wide range of technology. This includes access to:
    - Computers, laptops, tablets and other digital devices

    - Internet, which may include search engines and educational websites
    - Learning platform/intranet
    - Email
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use appropriate search tools as identified following an informed risk assessment.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to learner's age and ability.
    - **Early Years Foundation Stage and Key Stage 1**
        - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learner's age and ability.
    - **Key Stage 2**
        - Learners will use age-appropriate search engines and online tools.
        - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learner's age and ability.

7.2 Managing internet access

- All staff, learners and visitors will read and agree an acceptable use policy before being given access to our computer system, IT resources or the internet.

7.3 Filtering and monitoring

7.3.1 Decision making

- Borough Green Primary School Governors, IT technician 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.
- Our decision regarding filtering and monitoring has been informed by a risk assessment,considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- The Governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring

alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Appropriate filtering

- Borough Green Primary School's education broadband connectivity is provided through EiS.
- Borough Green Primary School uses:
    - Smoothwall which blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. 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.
    - is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
    - Smoothwall integrates the 'the police assessed list of unlawful terrorist content,produced on behalf of the Home Office'
- We work with EiS Kent IT to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners or staff discover unsuitable sites or material, they are required to inform the DSL and/or the IT technician.
- Filtering breaches will be reported to the DSL (or deputy) and technical staff and will berecorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

7.3.3 Appropriate monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices.
- All users will be informed that use of our systems can be monitored. All monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with UK General Data Protection Regulations and Data Protection legislation.

7.5 Security and management of information systems

- We take appropriate steps to ensure the security of our information systems, including:
    - Virus protection being updated regularly.
    - 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.

7.5.1 Password policy

- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 1 all learners are provided with their own unique username and passwords to access our systems; learners are responsible for keeping their password private.
- We require all staff to
    - use strong passwords for access into our system.
    - change their passwords every six weeks.
    - not share passwords or login information with others or leave passwords/login detailswhere others can find them.
    - not to login as another user at any time.
    - lock access to devices/systems when not in use.

7.6 Managing the safety of our website

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

7.7 Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance

with the associated policies, including (but not limited to) the cameras and image use, data protection ,acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones policies.

7.8 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including acceptable use of technology policies and the code of conduct/behaviour policy.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and unusual/harmful content will be reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the community will immediately tell the DSL if they receive offensive communication, and this will be recorded in our 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 on site.
- Staff must protect confidential documents with a password to be sent to the recipient separately.

7.8.1 Staff email

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

7.8.2 Learner email

- Where appropriate, learners will use a provided email account for educational purposes.
- Learners 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 will be used for communication outside of the setting.

7.9 Management of applications (apps) used to record children's progress

- We use Tapestry and Arbor to track learners' progress and share appropriate information with parents and carers.
- The Early Years leader will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the UK General Data Protection Regulations (GDPR) and Data Protection legislation.

- To safeguard learner's data:
    - only learner issued devices will be used for apps that record and store learners' 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 learners' personal details, attainment or images.
    - devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8 Social Media

Borough Green Primary School believes everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline, and all members of our community are expected to engage in social media in a positive and responsible manner.

All members of our community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

- We will restrict learner and staff access to social media via our filtering and monitoring systems which are applied to all Borough Green Primary School provided devices and systems; further information on how this is achieved in addressed in our child protection policy.
- The use of social media or apps, for example as a formal remote learning platform or education tool will be robustly risk assessed by the DSL and/or headteacher prior to use with learners. Any use will take place in accordance with our existing policies, for example, child protection, staff/learner behaviour acceptable use policies and the remote learning Acceptable Use Policy.
- Concerns regarding the online conduct of any member of Borough Green Primary School community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including behaviour, staff code of conduct, Acceptable Use Policies, and child protection.

8.1 Staff use of social media

- The use of social media during Borough Green Primary School hours for personal use is not permitted for staff.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct policy and acceptable use of technology policy.
- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.

- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection, whistleblowing and complaints policies.

8.2 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the Borough Green Primary School. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media. This may include, but is not limited to:
    - Setting appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the school.
- Members of staff are encouraged not to identify themselves as employees of Borough Green Primary School on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- 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 children 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.

8.3 Communicating with children and their families

- Staff will not use any personal social media accounts to contact children or their family members.
- All members of staff are advised not to communicate with or add any current or past pupils or their family members, as ‘friends’ on any personal social media accounts.
- Any communication from children and parents/carers received on personal social media accounts will be reported to the DSL (or deputy) and/or the headteacher.
- Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the DSL and the headteacher. Decisions made and advice provided in these situations will be formally recorded to safeguard children, members of staff and the setting.
- If ongoing contact with pupils is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

8.4 Children's use of social media

- The use of social media during school hours for personal use is not permitted for children.
- Many online behaviour incidents amongst children and young people occur on social media outside the school day and off the school premises. Parents/carers are responsible for this behaviour; however, some online incidents may affect our culture and/or pose a risk to children's health and well-being. Where online behaviour online poses a threat or causes harm to another child, could have repercussions for the orderly running of the school when the child is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our behaviour and child protection/online safety policies.
- Borough Green Primary School will empower our children to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to children as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection policy and the RSE policy.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for children under the required age as outlined in the services terms and conditions.
- Children will be advised:
    - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
    - to only approve and invite known friends on social media sites and to deny access to others, for example by making profiles private.
    - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so 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.
    - how to report concerns on social media, both within the setting and externally.
- Any concerns regarding children's use of social media will be dealt with in accordance with appropriate existing policies, including child protection and behaviour.
- The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.
- Sanctions and/or pastoral support will be implemented and offered to children as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.
- Concerns regarding children's use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

8.5 Policy monitoring and review

- Technology evolves and changes rapidly. Borough Green Primary School will review this policy at least annually. The policy will 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. Any issues identified will be incorporated into our action planning.
- All members of the community will be made aware of how the school will monitor policy compliance: in safeguarding training, staff meetings and through sharing of policies.

8.6 Responding to policy breaches

- All members of the community are informed of the need to report policy breaches or concerns in line with existing school policies and procedures. This includes the staff code of conduct, the whistleblowing policy, child protection and the behaviour policy.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- We require staff, parents/carers and children to work in partnership with us to resolve issues.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Children, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or headteacher will seek advice from Kent County Councils Education Safeguarding Service or other agency in accordance with our child protection policy.

9 Remote Learning

- Appropriate risk assessments to ensure safer use will be carried out prior to setting online home learning.
- Parents will be informed of what remote learning asks children to do (including which sites they will be advised to access) and will be told how to keep their child safe online by using filtering and monitoring.
- Parents will also be informed about any school staff their child will interact with online.

10 Safe use of mobile and smart technology expectations

- Borough Green Primary School recognises that use of mobile and smart technologies is part of everyday life for many children, staff and parents/carers.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of our community are advised to:
    - take steps to protect their personal mobile phones or other smart devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

    - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on personal phones or devices.
- Mobile devices and other forms of smart technology are not permitted to be used in specific areas on site; this includes classrooms, changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content, including via personal mobile devices and/or smart technology is forbidden by any member of the community; any breaches will be dealt with in line with our behaviour and child protection policies and the staff code of conduct.
- All members of the Borough Green Primary School community are advised to ensure that their personal mobile and smart technology devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

10.1 School provided devices

- Staff providing formal remote/online learning will do so using Borough Green Primary School provided equipment in accordance with our Acceptable Use Policy (AUP)/remote learning AUP.
- Borough Green Primary School devices will be suitably protected via a password and must only be accessed or used by members of staff and children.
- Borough Green Primary School devices will always be used in accordance with our staff code of conduct, behaviour policy, acceptable use of technology policy and other relevant policies.
- Where staff and children are using Borough Green Primary School provided devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.

10.2 Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones, wearable technology and other mobile/smart devices, will take place in accordance with the law, as well as relevant Borough Green Primary School policy and procedures, including child protection, data protection and GDPR policy, staff code of conduct and Acceptable Use Policies.
- Staff will be advised to:
    - Keep personal mobile and smart technology devices in a safe and secure place during lesson time.
    - Keep personal mobile phones and devices switched off or set to ‘silent’ or ‘do not disturb’ modes during lesson times.
    - Ensuring that mobile phones or personal devices are not used or on display where children are present. Staff are permitted to wear “smart watches” or any other wearable technology with calling, messaging, tracking or recording functions but are asked to treat them like mobile phones and refrain from using them when they are supervising children.
    - Ensure that Bluetooth or other forms of communication, such as ‘airdrop’, are hidden or disabled during lesson times.

    - Not use personal mobile or smart technology 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 personal mobile and smart technology devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal mobile and smart technology devices for contacting children or parents and carers.
    - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL and headteacher.
- Staff will only use Borough Green Primary School provided equipment (not personal devices):
    - to take photos or videos of children in line with our image use policy.
    - to work directly with children during lessons/educational activities.
    - to communicate with parents/carers.
- Where remote learning activities take place, staff will use Borough Green Primary School provided equipment. If this is not available, staff will only use personal devices with prior approval from the headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy.
- If a member of staff breaches our policy, action will be taken in line with our staff code of conduct, child protection policy and whistleblowing policy.
- If a member of staff is thought to have illegal content saved or stored on a personal mobile or other device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted, and the LADO (Local Authority Designated Officer) will be informed in line with our whistleblowing policy and Code of Conduct.

10.3 Children's use of mobile and smart technology

- Children will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.
- Safe and appropriate use of mobile and smart technology will be taught to children as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection policy and relevant specific curriculum policies such as the RSE policy.

    - Children are not permitted to use personal mobile or smart devices whilst on the school site, this includes the wearing of "smart watches" or other or any other wearable technology with calling, messaging, tracking or recording functions. Where these are required, for example for safety reasons when children are transporting to and from school, devices should be turned off and handed into the school office in the morning. They can then be collected at the end of day.
- Borough Green Primary School expects children's personal mobile or smart technology devices to be kept safe and secure when on site. This means:
    - handing into the school office at the start of day.
    - If a child needs to contact their parents or carers whilst on site, office staff will do this for them on a Borough Green Primary School phone.

- Parents are advised to contact their child via the Borough Green Primary School office
- If a child requires access to personal mobile or smart technology devices in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the headteacher prior to use being permitted.
    - Any arrangements regarding access to personal mobile or smart technology devices in exceptional circumstances will be documented and recorded by the Borough Green Primary School.
    - Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the learner and their parents carers before use is permitted.
- Where children's personal mobile or smart technology devices are used when learning at home, this will be in accordance with our Acceptable Use Policy.
- Personal mobile or smart technology devices must not be taken into statutory assessments. Children found in possession of a mobile phone or personal device which facilitates communication or internet access during a statutory assessment will be reported to the appropriate body.

10.4 Searching, screening and confiscation of electronic devices

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.
- Where there are any concerns regarding children's use of mobile or smart technology or policy breaches, they will be dealt with in accordance with our existing policies, including child protection, online safety and behaviour.
- Staff may confiscate a child's personal mobile or smart technology device if they believe it is being used to contravene our child protection or behaviour policy.
- Personal mobile or smart technology devices that have been confiscated will be held in a secure place in the school office and released to parents/carers at the end of the day.
- Where a concern involves a potentially indecent image or video of a child, staff will respond in line with our child protection policy and will confiscate devices, avoid looking at any content, and refer the incident to the Designated Safeguarding Lead (or deputy) urgently as they will be most appropriate person to respond.
- If there is suspicion that data or files on a child's personal mobile or smart technology device may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation
- If deemed to be necessary and appropriate, searches of personal mobile or smart technology devices may be carried out in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance.

- Staff will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a pupil's electronic device that they reasonably suspect are likely to put a person at risk.
- The Designated Safeguarding Lead (or deputy) will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a pupil was in possession of prohibited items, as identified in our behaviour policy.
- The Designated Safeguarding Lead (or deputy) will be involved without delay if staff believe a search of a pupil's personal mobile or smart technology device has revealed a safeguarding risk.
- In exceptional circumstances and in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so.
    - In determining whether there is a 'good reason' to examine images, data or files, the headteacher or an authorised member of staff will need to reasonably suspect that the images, data or files on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
    - In determining whether there is a 'good reason' to erase any images, data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable.
    - If the data or files are not suspected to be evidence in relation to an offence, the headteacher or an authorised member of staff may delete the images, data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.
- If the headteacher or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

10.5 Visitors' use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:
    - mobile phones are not to be used or on display where children are and are only permitted within specific areas or are only permitted for specific purpose, for example, as part of multi-agency working arrangements.
- Appropriate signage and information are in place (see laminated information sheets with the Visitors' signing in book) to inform visitors of our expectations for safe and appropriate use of personal mobile or smart technology; visitors are given copies of the BGPS Safeguarding Leaflet and the Visitors AUP (which should be read, and signed) on arrival.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection.

- If visitors require access to mobile and smart technology, for example when working with children as part of multi-agency activity, this will be discussed with the headteacher prior to use being permitted.
    - Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the Borough Green Primary School. This may include undertaking appropriate risk assessments if necessary.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or headteacher of any breaches of our policy.

10.6 Responding to policy breaches and Online Safety Incidents

10.61 Concerns about learner online behaviour and/or welfare

- The DSL (or deputy) will be informed of all online safety concerns involving safeguarding orchild protection risks in line with our child protection policy.
- All concerns about learners will be recorded in line with our child protection policy.
- Borough Green Primary School 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.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported torelevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners asappropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, asand when required.

10.62 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the Headteacher, in accordance with ourallegations against staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO(Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staffcode of conduct.
- Welfare support will be offered to staff as appropriate.

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

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the Headteacher. The Headteacher will respond to concerns in line with existing policies, including but not limited to child protection, 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 Concerns

11.1 Online sexual violence and sexual harassment between children

- Our DSL and appropriate members of staff have accessed and understood the DfE "Sexualviolence and sexual harassment between children in schools and colleges" (2018) guidanceand part 5 of 'Keeping children safe in education' 2022.
    - Full details of our response to child on child abuse, including sexual violence and harassment can be found in our child protection policy.
- Borough Green Primary School recognises that sexual violence and sexual harassmentbetween 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 withoutthem knowing, with the intention of obtaining sexual gratification, or causing the victimhumiliation, 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 ourequipment.
- If made aware of any concerns relating to online sexual violence and sexual harassment, wewill:
    - immediately notify the DSL (or deputy) and act in accordance with our child protectionand behaviour policy.
    - if content is contained on learners personal devices, they will be managed inaccordance with the DfE 'searching screening and confiscation' advice.
    - provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing onlinecontent, and 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 beingmanaged.
    - if appropriate, make referrals to partner agencies, such as Children's Social WorkService and/or the police.
    - if the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguardingaction is taken in the wider local community.

    - If a criminal offence has been committed, the DSL (or deputy) will discuss thiswith 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.
- Borough Green Primary School recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Borough Green Primary School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Borough Green Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- Staff will be made aware of sources of support regarding online sexual violence and sexual harassment between learners.

11.2 Youth produced sexual imagery ("sexting")

- Borough Green Primary School recognises youth produced sexual imagery (also 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 schoolsand colleges: responding to incidents and safeguarding young people' and the local KSCMP 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.
- Borough Green Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of ageand ability appropriate educational methods.
- Staff will be made aware of sources of support regarding the taking and sharing of 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 suspected youth produced sexual imagery, unless there is no other option, orthere is a clear safeguarding need or reason to do so.
        - If it is deemed necessary, the imagery will only be viewed where

possible bythe DSL, 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 (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 local procedures.
    - ensure the DSL (or deputy) responds in line with the UKCIS and KSCMP guidance.
    - Store any devices containing potential youth produced sexual imagery securely
        - If content is contained on learners personal devices, they will be managed inaccordance with the DfE 'searching screening and confiscation' advice.
        - If a potentially indecent image has been taken or shared on our network ordevices, we will act to block access to all users and isolate the image.
    - carry out a risk assessment in line with the UKCIS (UK Council for Child Internet Safety) and KSCMP guidance which considers the age and vulnerability of learners involved, including the possibility of 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 and/or the police, as deemed appropriate in line with the UKCIS and KSCMP 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 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; theleadership team will also review and update any management procedures, where necessary.

11.3 Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- Borough Green 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.
- We will implement preventative approaches for online child abuse and exploitation via arange of age and ability appropriate education for learners,

staff and parents/carers.

- We will ensure that all members of the community are aware that CCE can be facilitated through the use of technology, for example gangs may target young people via social media or provide devices in exchange for or to support criminal activity.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies and the relevant KSCMP procedures.
    - store any devices containing evidence securely.
        - If content is contained on learners' personal devices, they will be managed inaccordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner 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 and provide support and signposting, as appropriate.
    - 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 abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, foor example if the concern relates to online sexual abuse via CEOP: 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 Service and/or police.
- If made aware of intelligence or information which may relate to child sexual exploitation (onor offline), it will be passed through to the police by the DSL (or deputy).
- If members of the public or learners at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- Borough Green Primary School will ensure staff are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- We will respond to concerns regarding Indecent and Prohibited Images of Children (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 (IWF) block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant KSCMP procedures.
    - store any devices involved securely.
    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been inadvertently exposed toindecent images of children, we will:
    - ensure that the DSL (or deputy) is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images arereported to the IWF 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 arereported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 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) following a written request from the police.
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children onschool provided devices, we will:
    - ensure that the Headteacher is informed in line with our whistleblowing policy and Staff Code of Conduct.
    - inform the **Local Authority Designated Officer** (LADO) and other relevant organisations in accordance with our whistleblowing policy and Staff Code of Conduct.
    - quarantine any devices until police advice has been sought.

11.5 Cyber-bullying

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Borough GreenPrimary School.
- Children will be taught what cyber-bullying is and what to do if they think it is happening to them or are aware that it is happening to someone else.
- Cyber bullying will be part of discussions of bullying and online safety in computing lessons, PHSE, RSE and in general classroom discussions in response to incidents or questions.
- Staff are aware that cyberbullying can be considered as emotional abuse and are taught about it in annual safeguarding training and staff updates
- 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.
-

11.6 Online hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Borough Green Primary School and will be responded to in line with existing policies, including child protection 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, theDSL (or deputy) will obtain advice through the Education Safeguarding Service and/or the police.

11.7 Online radicalisation and extremism

- As listed in this policy, 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 learner or adult may be at risk of radicalisation online, the DSL (ordeputy) 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 whistleblowing policies.

11.8 Staff Training on Specific Online Concerns

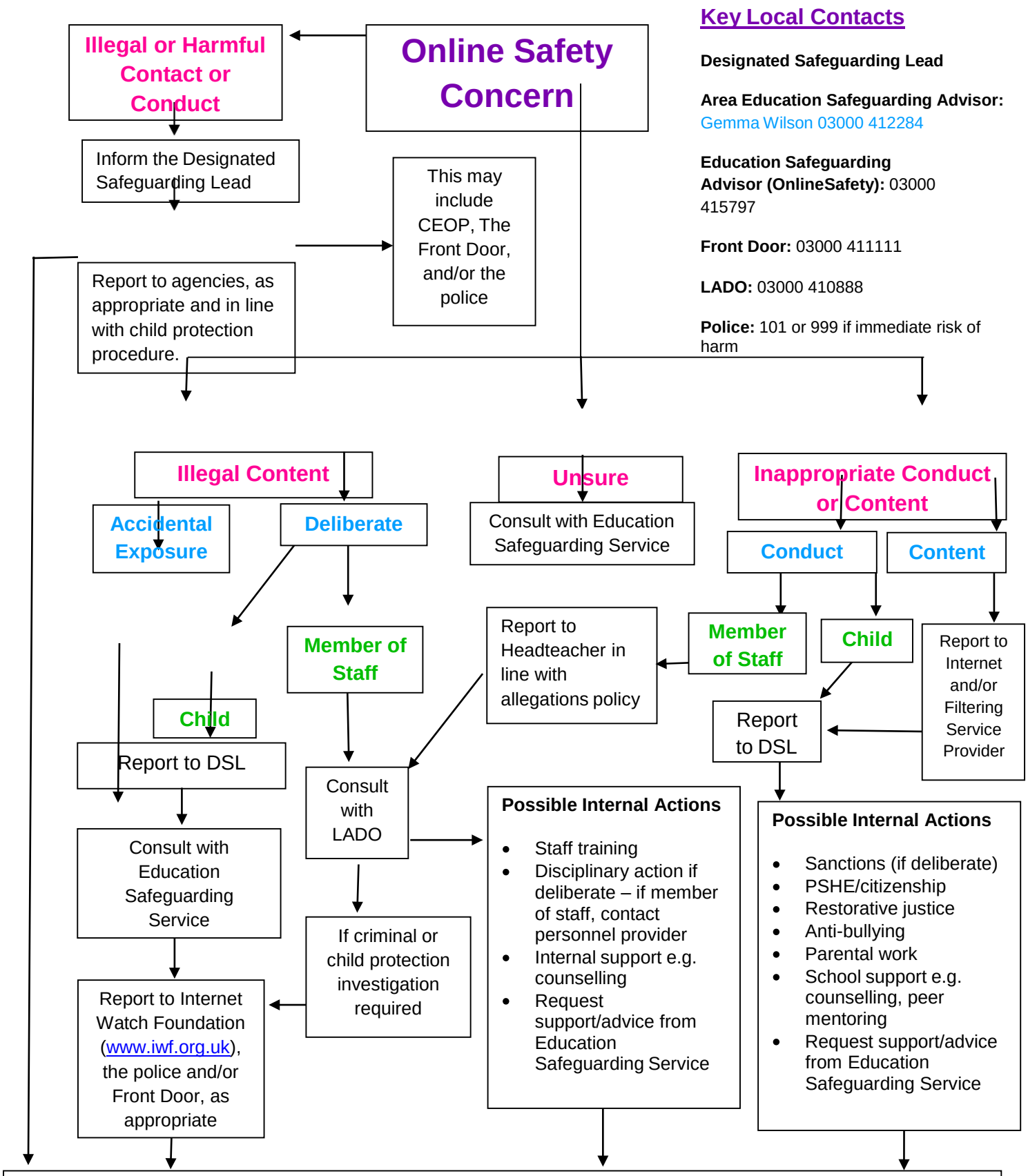
As part of safeguarding training (including in updates, e-bulletins, and staff meetings) all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

Responding to an Online Safety Concern Flowchart



Key Local Contacts

Designated Safeguarding Lead

Area Education Safeguarding Advisor: Gemma Wilson 03000 412284

Education Safeguarding Advisor (OnlineSafety): 03000 415797

Front Door: 03000 411111

LADO: 03000 410888

Police: 101 or 999 if immediate risk of harm

Useful Links

Kent Educational Setting Support and Guidance

Education Safeguarding Service, The Education People:

- 03000 415797
    - Rebecca Avery, Education Safeguarding Advisor (Online Protection)
    - Ashley Assiter, Online Safety Development Officer
- Guidance for Educational Settings:
    - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and- safeguarding
    - www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCMP: www.kscb.org.uk

Kent Police:

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

Front Door:

- The Front Door can be contacted on 03000 41 11 11
- Out of hours (after 5pm / Urgent calls only) please contact: 03000 41 91 91

Early Help and Preventative Services: www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

Other:

- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eisit.uk

National Links and Resources for Settings, Learners andParents/carers

- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk

- Internet Watch Foundation (IWF): www.iwf.org.uk

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety

- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
  - Report Harmful Content: https://reportharmfulcontent.com/

- 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

- Internet Matters: www.internetmatters.org

- Parent Zone: https://parentzone.org.uk

- Parent Info: https://parentinfo.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk

- Lucy Faithfull Foundation: www.lucyfaithfull.org

- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

- Action Fraud: www.actionfraud.police.uk

- Get Safe Online: www.getsafeonline.org

- DfE https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes
- https://learning.nspcc.org.uk/news/covid/undertaking-remote-teaching-safely
- The Education People: Think before you scare
- UK Safer Internet Centre: De-escalating and responding to harmful online challenges
- London Grid for Learning: Parents – scare or prepare?