Lamberhurst St Mary's CEP (VC) School

Online Safety

(Taken from the KCC Model Policy, September 2021)

6th Edition

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. Any amendments will require the approval of the full Governing Body. A copy is stored online in the Teacher Area of the school server.

Designated Safeguarding Lead (s):	Mrs C Bromley, Headteacher
	Mrs N Mitchell, Deputy Headteacher
	Mrs G Turner-Moore, Senior Teacher
Named Governor with lead responsibility:	Mrs L Denning, Safeguarding Governor

Date of approval by Governing Body	11 October 2021
Signature of Chair of Governors	Mr P Edgesmith
Signature of Headteacher	Mrs C Bromley
Date Due for review	Autumn term 2022

Disclaimer
The Education People and the leadership of Lamberhurst St Mary's Primary School make every effort to ensure that the information in this document is accurate and up to date. If errors are brought to our attention, we will correct them as soon as practicable.

Lamberhurst St Mary’s School Online Safety Policy

1. Policy Aims

- This policy has been written by Lamberhurst St Mary’s School, involving staff, pupils and parents/carers, building on the Kent County Council (KCC)/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” 2021, Early Years and Foundation Stage 2017, ‘Working Together to Safeguard Children’ 2018 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 pupils 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.
- Lamberhurst St Mary’s School 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.
- This policy applies to pupils, parents/carers and 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).
- Lamberhurst St Mary’s School identifies that the internet and technology, including computers, tablets, mobile phones, smart watches, games consoles and social media, is an important part of everyday life and presents positive and exciting opportunities, as well as challenges and risks. This policy applies to all access to and use of technology, both on and off-site
- This policy links with several other policies, practices and action plans including but not limited to:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and/or the Code of conduct/Staff Behaviour Policy
    - Behaviour and discipline policy
    - Child protection policy
    - Confidentiality policy
    - Curriculum policies, such as: Computing, Personal Social & Health Education (PSHE), and Relationships, Health (and Sex) Education (R(S)HE)
    - Data security
    - Image use policy
    - Mobile and Smart Technology policy
    - Social Media policy
    - Remote Learning policy

2. Responding to Emerging Risks

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

3. Monitoring and Review

- Lamberhurst St Mary's School will review this policy at least annually. The policy will also be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, 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.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Mrs C Bromley, Headteacher, is recognised as holding overall lead responsibility for online safety, however Lamberhurst St Mary's School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.
- Trained additional DSLs are: Mrs N Mitchell, Deputy Headteacher, and Mrs G Turner-Moore, Senior Teacher.
- The Online safety lead for the Governing Body is: Mrs L Denning, Local Authority Governor.

4.1 The leadership and management team will:

- Create a whole school culture that incorporates online safety throughout all elements of school life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with IT support to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.

- Ensure robust reporting channels are in place for the school 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, 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 school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues
- Liaise with other members of staff or other agencies on matters of online safety.
- Ensure 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 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 pupils safe online, including 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. (See Child Protection / Safeguarding file).
- 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) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

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

- Contribute to the development of our online safety policies.
- Read and adhere to our 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/or deputy) and signposting pupils, parents and 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 (including KCC EIS) to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures (including password policies and encryption) as directed by the leadership team 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.

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

- Engage in and apply 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 to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforce appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement and/or acceptable use policies.
- Seek help and support from the 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 (including PTA sites), safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies that their children access and use at home.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- Lamberhurst St Mary's school will establish and will empower our learners to acquire the knowledge needed to use the technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- We and will raise awareness and promote safe and responsible internet use amongst learners by:
    - Ensuring our curriculum and school approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance.
    - Ensuring online safety is addressed in the PSHE, R(S)HE and Computing programmes of study
    - Reinforcing online safety principles in other curriculum subjects and whenever technology or the internet is used on site.
    - Implementing appropriate peer education approaches.
    - Creating a safe environment in which all pupils 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 pupils who may be impacted by the content.
    - Making informed decisions to ensure that any educational resources used are appropriate for our pupils.
    - Using external visitors, where appropriate, to complement and support our internal online safety education approaches
    - Providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
    - Rewarding positive use of technology.
- Lamberhurst St Mary's school will support pupils to read and understand our acceptable use policies in a way which suits their age and ability by:
    - Sharing our acceptable use policies with them in accessible and appropriate ways.
    - 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.
    - Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Lamberhurst St Mary's school will ensure pupils 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.
    - Enabling them to understand what acceptable and unacceptable online behaviour looks like.
    - Teaching pupils 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.
    - preparing them to identify possible online risks and make informed decisions about how to act and respond.

    - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Pupils

- Lamberhurst St Mary's School recognises that any pupil can be vulnerable online, and vulnerability can fluctuate depending on age, developmental stage and personal circumstances. However, there are some pupils, for example looked after children and those with special educational needs or disabilities, who may be more susceptible or may have less support in staying safe online.
- Lamberhurst St Mary's School will ensure that differentiated and appropriate online safety education, access and support is provided to all pupils who require additional or targeted support.
- Staff at our school will seek input from specialist staff as appropriate, including the DSL, SENCO and Child in Care Designated Teacher 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, including our acceptable use policy, with all members of staff as part of induction.
- Provide up-to-date and appropriate training for all staff which is integrated, aligned and considered as part of our overarching safeguarding approach.
    - This will be achieved as part of existing safeguarding and child protection training/updates.
    - This will cover the potential risks posed to pupils (Content, Contact and Conduct) 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.
- Ensure staff are 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.
- Ensure staff are 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 pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving pupils, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- Lamberhurst St Mary's School recognises that parents and carers have an essential role to play in enabling our pupils to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - Drawing their attention to our online safety policy and expectations in newsletters, letters and on the school's website.

    - Requesting parents and carers read online safety information as part of joining Lamberhurst St Mary's School.
    - Requiring parents and carers to read our acceptable use of technology policies and discuss its implications with their children.

6. Safer Use of Technology

6.1 Classroom Use

- Lamberhurst St Mary's 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
    - 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 our acceptable use of technology policies and with appropriate safety and security measures in place. All school devices are linked to the school server which is monitored by ICT technical manager and KCC EIS.
- 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 (sites include SWGfL Squiggle, Google Safe Search or CBBC safe search), following an informed risk assessment, to identify which tool best suits the needs of our community.
- The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to pupils' 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.
        - Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

6.2 Managing Internet Access

- We 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.

6.3 Filtering and Monitoring

6.3.1 Decision Making

- Lamberhurst St Mary's 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.
- Lamberhurst St Mary's 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. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- 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 pupils; effective classroom management and regular education about safe and responsible use is essential.

6.3.2 Appropriate Filtering

- Lamberhurst St Mary’s School’s educational broadband connectivity is provided through KPSN.
- We use 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.
- We work with KCC and the school’s broadband team or broadband/filtering provider to ensure that our filtering policy is continually reviewed.
- The school has a clear procedure for reporting filtering breaches.
  - If pupils discover unsuitable sites, they will be required to 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 access to material believed to be illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police and/or CEOP.

6.3.3 Appropriate Monitoring

- We will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by physical monitoring (supervision), monitoring internet and web access.
- 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 behaviour and allegations policy

6.4 Managing Personal Data Online

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

    - Full information can be found in our Data Protection policy, a copy of which is available from the school office.

6.5 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 but the youngest users.
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - All devices are linked to the school server. Further information about technical environment safety and security can be found in the AUP.
    - We will review the effectiveness of our security approaches and procedures periodically in order to keep up with evolving cyber-crime technologies

6.5.1 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 1, 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.
    - 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.

6.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or 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.

- We will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

6.7 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, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

6.8 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, 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 reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- School email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the school community will immediately tell Mrs C. Bromley, the Designated Safeguard Lead, 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.
- Email sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper would be.

6.8.1 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 school 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 pupils and parents.

6.8.2 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.

6.9 Educational use of Videoconferencing and/or Webcams

- Lamberhurst St Mary’s School recognises 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.
    - Videoconferencing contact details will not be posted publicly.

  - 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.

6.9.1 Users

- Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the pupils' age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- 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.

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

6.10 Management of Learning Platforms

- Lamberhurst St Mary's School does not currently have a school learning platform.

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

- We use our own in-school generated system of School Tracking Sheets and Venn Diagrams to track pupils' progress and share appropriate information with parents and carers. Information is shared with parents three times per year at Parent Consultation meetings, a Mid-Year report in February, and an End of Year Report in July.
- The Headteacher will ensure that the use of tracking systems to track pupil progress is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- 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.

6.12 Management of Remote Learning

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

- Lamberhurst St Mary's School will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.
- All communication with learners and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and/or agreed systems e.g. Microsoft 365.
- Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.
- Staff and pupils 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 pupils 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. Lamberhurst St Mary's School will continue to be clear who from the school their child is going to be interacting with online.
- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

7. Responding to Online Safety Incidents and Concerns

- All members of the school 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.
    - are informed of the need to report policy breaches or concerns in line with existing school policies and procedures.
    - will respect confidentiality and the need to follow the official procedures for reporting concerns.
    - will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
    - will be made aware of how the school will monitor policy compliance by: acceptable use policies, staff training and classroom management.
    - are expected to adopt a partnership with the school to resolve issues.
- If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the local authority or other agency in accordance with our child protection policy
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm.

- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local schools are involved or the wider public may be at risk, the DSL and headteacher will speak with the police and/or the Local Authority first, to ensure that potential criminal or child protection investigations are not compromised

7.1 Concerns about Pupils Online Behaviour and/or Welfare

- All concerns about pupils will be responded to and recorded in line with our child protection policy:
    - The DSL (or deputy) will be informed of any online safety concerns involving safeguarding or child protection concerns in line with our child protection policy.
    - The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be implemented and/or offered to pupils as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents and carers of any incidents or concerns involving their child, as and when required.

7.2 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 DSL and dealt with 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.
- Where appropriate, welfare support will be offered, and where necessary, civil and/or legal action may be taken.

7.3 Concerns about staff online behaviour and/or welfare

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

8. Procedures for Responding to Specific Online Incidents or Concerns

8.1 Online Peer on Peer Abuse

- Lamberhurst St Mary's School recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.
- We recognise that online peer on peer 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.
- Lamberhurst St Mary's School 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.
- Lamberhurst St Mary's School believes that all staff have a role to play in challenging inappropriate online behaviours between peers.
- Lamberhurst St Mary's School recognises that, even if there are no reported cases of online peer on peer abuse, such abuse is still likely to be taking place.
- Concerns about pupils' behaviour, including peer on peer 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.
- Lamberhurst St Mary's School want children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online peer on peer 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. Pupils who experience abuse will be offered appropriate support, regardless of where the abuse takes place.

8.1.1 Child on Child Online Sexual Violence and Sexual Harassment

- When responding to concerns relating to online child on child sexual violence or harassment, Lamberhurst St Mary's School 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.
- Lamberhurst St Mary's School 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.
- Lamberhurst St Mary’s School 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.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- Lamberhurst St Mary’s 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 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 the Education Safeguarding Service, 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:
- If made aware of online sexual violence and sexual harassment, we 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.

- o review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

- Lamberhurst St Mary's School 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. We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

8.1.2 Nude or semi-nude image sharing

- Lamberhurst St Mary's School 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, <School name> 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'
- Lamberhurst St Mary's School 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 policy and the relevant local procedures and 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 Education Safeguarding Service.
  - Store any devices securely:
    - if content is contained on pupils 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 the school network or devices, we will take action 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.
  - 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.

8.1.3 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Lamberhurst St Mary's School.
- Full details of how we will respond to cyberbullying are set out in our Anti-bullying policy, a copy of which is available on the school website.

8.2 Online Child Sexual Abuse and Exploitation

- Lamberhurst St Mary's 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.

- Lamberhurst St Mary's 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 pupils, and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for pupils, staff and parents/carers.
- 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.
- The school will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible on the school website and available to pupils and other members of the community.
- If we are made aware of incident involving online child sexual abuse and/or exploitation, we will:
    - Act in accordance with our Child protection policies and the relevant Kent Safeguarding Child Board's procedures.
    - Store any devices containing evidence securely.
        - If content is contained on pupils' personal devices, they will be managed in accordance 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 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.
    - 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.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our school premises or using school provided or personal equipment.
    - Where possible and appropriate, pupils will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via the National Crime Agency CEOP Command (NCA-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 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 police by the DSL (or Deputy).
- If members of the public or pupils at other schools are believed to have been targeted, the DSL (or Deputy) will seek support from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

8.3 Indecent Images of Children (IIOC)

- Lamberhurst St Mary's School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate.

- We will respond to concerns regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- We will take action 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 Kent Safeguarding Child Boards procedures.
    - Store any devices involved securely until advice has been sought. If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice..
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF) and police.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk and/or police.
    - inform the police as appropriate, for example if images have been deliberately sent to or shared by pupils.
    - report concerns, as appropriate, to parents and carers.
- If we are made aware that indecent images of children have been found on the school provided devices, we will:
    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the 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 and carers.
- If we are made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
    - Ensure that the Headteacher is informed in line with our managing allegations against staff policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations against staff policy.
    - Quarantine any devices until police advice has been sought.

8.4 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Lamberhurst St Mary's School and will be responded to in line with existing school policies, including Child Protection, 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 we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or the police.

8.5 Online Radicalisation and Extremism

- As listed in this policy we will take all reasonable precautions to ensure that children and staff are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which takes into account the needs of pupils.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately and action will be taken in line with our Child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies.

8.6 Cybercrime

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

Responding to an Online Safety Concern Flowchart

Key Local Contacts

Designated Safeguarding Lead (s):
Mrs Caroline Bromley, Headteacher,
Mrs N Mitchell, Deputy Headteacher
Mrs G Turner-Moore, Senior Teacher
Headteacher@lamberhurst.kent.sch.uk
Tel: 01892 890281

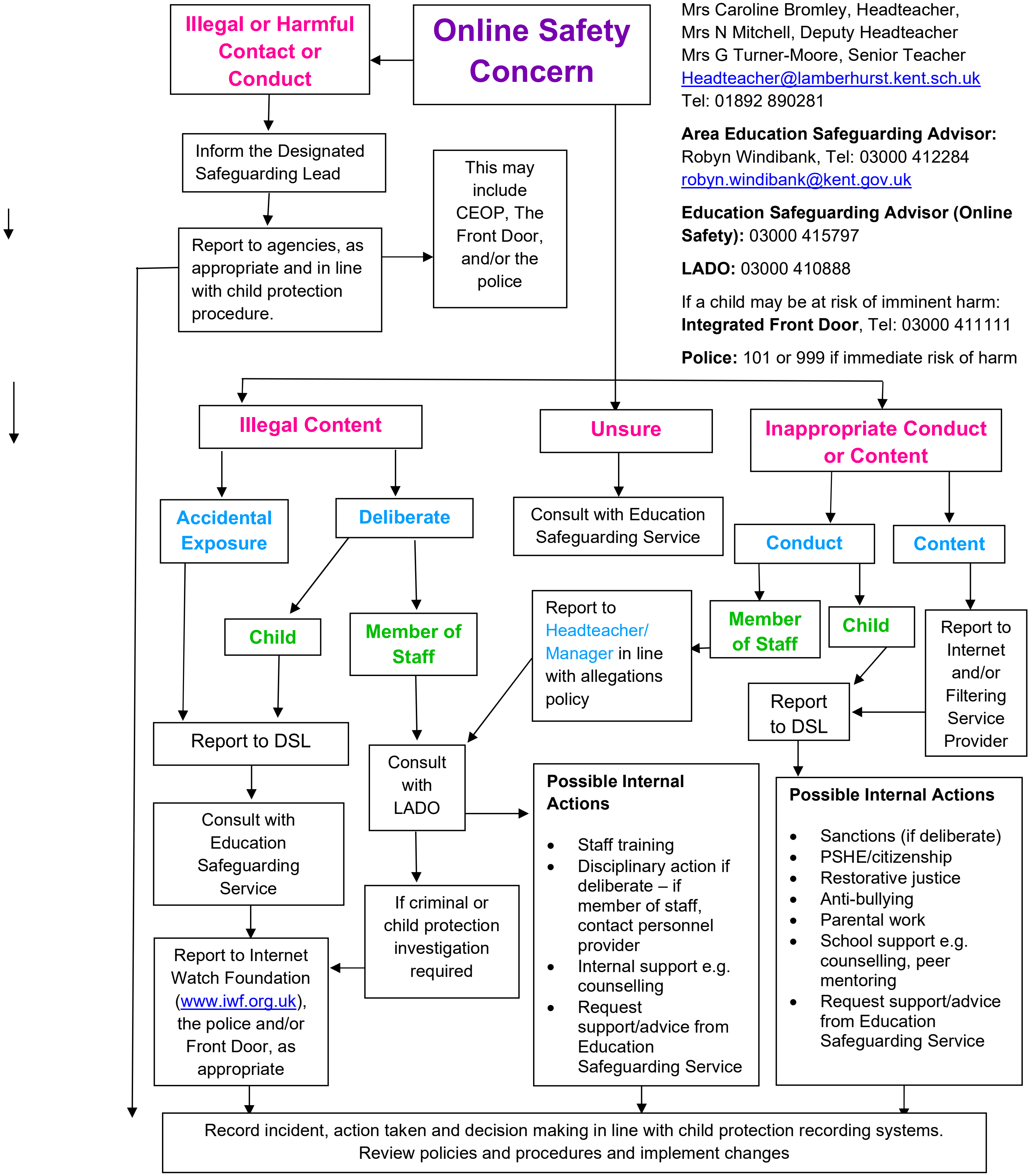
Area Education Safeguarding Advisor:
Robyn Windibank, Tel: 03000 412284
robyn.windibank@kent.gov.uk

Education Safeguarding Advisor (Online Safety): 03000 415797

LADO: 03000 410888

If a child may be at risk of imminent harm:
Integrated Front Door, Tel: 03000 411111

Police: 101 or 999 if immediate risk of harm



Online Safety Concern

Illegal or Harmful Contact or Conduct

Inform the Designated Safeguarding Lead

Report to agencies, as appropriate and in line with child protection procedure.

This may include CEOP, The Front Door, and/or the police

Illegal Content

Accidental Exposure

Deliberate

Child

Member of Staff

Report to DSL

Consult with Education Safeguarding Service

Consult with LADO

If criminal or child protection investigation required

Report to Internet Watch Foundation (www.iwf.org.uk), the police and/or Front Door, as appropriate

Unsure

Consult with Education Safeguarding Service

Inappropriate Conduct or Content

Conduct

Content

Member of Staff

Child

Report to Headteacher/ Manager in line with allegations policy

Report to DSL

Report to Internet and/or Filtering Service Provider

Possible Internal Actions

- Staff training
- Disciplinary action if deliberate – if member of staff, contact personnel provider
- Internal support e.g. counselling
- Request support/advice from Education Safeguarding Service

Possible Internal Actions

- Sanctions (if deliberate)
- PSHE/citizenship
- Restorative justice
- Anti-bullying
- Parental work
- School support e.g. counselling, peer mentoring
- Request support/advice from Education Safeguarding Service

Record incident, action taken and decision making in line with child protection recording systems.
Review policies and procedures and implement changes

Useful Links

Kent Educational School Support and Guidance

Education Safeguarding Service, The Education People:

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

KSCMB: 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 other 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:

- Kent Public Service Network (KPSN): www.kpsn.net
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

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