Lamberhurst St Mary's CEP (VC) School

Online Safety

(Taken from the KCC Model Policy, September 2019)

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 J Tobin, Safeguarding Governor

Date of approval by Governing Body	9 November 2020
Signature of Chair of Governors	Mr P Edgesmith
Signature of Headteacher	Mrs C Bromley
Date Due for review	Autumn term 2021

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.

Table of Contents

Online Safety Policy Content

Lamberhurst St Mary's School Online Safety Policy

1. Policy Aims

- This online safety 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" 2020, Early Years and Foundation Stage 2017, 'Working Together to Safeguard Children' 2018 and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.
- The purpose Lamberhurst St Mary's School online safety policy is to:
    - safeguard and protect all members of Lamberhurst St Mary's 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 use when responding to online safety concerns.
- Lamberhurst St Mary's 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.

2. Policy Scope

- Lamberhurst St Mary's School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- Lamberhurst St Mary's 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.
- Lamberhurst St Mary's School will empower our pupils 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 the school (collectively referred to as 'staff' in this policy) as well as pupils and parents and carers.
- This policy applies to all access to the internet and use of technology, including mobile technology, or where pupils, staff or other individuals have been provided with school issued devices for use off-site.

2.2 Links with other policies and practices

- This policy links with a number of 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 Sex and Relationships Education (SRE)
    - Data security
    - Image use policy
    - Mobile Technology and Social Media policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. Lamberhurst St Mary's 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 the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified via monitoring policy compliance will be incorporated into the school's action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Mrs C Bromley, Headteacher, has lead responsibility for online safety.
- 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 J Tobin, 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.
- 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.
- The leadership team will support all 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 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 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 knowledge and up to date required to keep pupils safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that pupils 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 the online safety policy and acceptable use of technology policies.
- Take responsibility for the security of school IT systems and the electronic data they use, or have access to.
- Model good practice when using technology, particularly 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.
- 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

- The school will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst pupils 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, SRE and Computing programmes of study
    - Reinforcing online safety principles in other curriculum subjects as appropriate, 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 vetted 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:
  - 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.
  - 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.
  - 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.

5.1.1 Vulnerable Pupils

- Lamberhurst St Mary's School recognises that any pupil can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some pupils, 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.
- Lamberhurst St Mary's School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable pupils.
- 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.

5.2 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedure 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.
    - 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, including curriculum, policies and procedures.
- Make staff aware that school IT systems are monitored, and that activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct, 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 ~~school~~ community.

5.3 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 children 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 that they read online safety information as part of joining Lamberhurst St Mary's School.
    - Requiring parents and carers to read the school AUP and discuss its implications with their children.

6. Reducing Online 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:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
    - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that 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.

- 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. This is clearly outlined in the school's acceptable use of technology policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 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
    - 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.

7.2 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.

7.3 Filtering and Monitoring

7.3.1 Decision Making

- 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.
- 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 pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- Lamberhurst St Mary's School uses educational broadband connectivity 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.

Dealing with Filtering breaches

- 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.

7.3.3 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 monitoring the DSL will respond in line with the child protection policy.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
    - Full information can be found in our Data Protection policy, a copy of which is available from the school office.

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 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.

7.5.1 Password policy

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

7.6 Managing the Safety of our Website

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

7.7 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated 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.

7.8 Managing Email

- Access to school email systems will always take place in accordance with data protection legislation and in line with other school policies, including: confidentiality, 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.

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 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.

7.8.2 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.

7.9 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.

7.9.1 Users

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

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

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If 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.

7.10 Management of Learning Platforms

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

7.11 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.

8. Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, peer on peer abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
    - Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Education Safeguarding Team.
- 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 as appropriate.
- Education Safeguarding Team or Kent 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 schools are involved or the wider public may be at risk, the DSL (or Deputy) will speak with the police or the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

8.1 Concerns about Pupils Welfare

- 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.
- All concerns about pupils will be recorded 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.
- We will inform parents and carers of any incidents or concerns involving their child, as and when required.

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

- Any complaint about staff misuse will be referred to the Headteacher, according with the Allegations 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 staff Behaviour policy and Code of conduct.
- Welfare support will be offered to staff as appropriate.

8.3 Concerns about staff online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the DSL (or deputy). The DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.

- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Online Sexual Violence and Sexual Harassment between Children

- Lamberhurst St Mary's School has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2020.
    - Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.
- Lamberhurst St Mary's School recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - non-consensual sharing of sexual images and videos,
    - sexualised online bullying,
    - online coercion and threats,
    - 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence.
    - unwanted sexual comments and messages on social media, and
    - online sexual exploitation.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on pupils' personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all pupils involved, such as implementing safety plans, offering on blocking, reporting and removing online content, 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 being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the police.
    - If the concern involves children and young people at a different educational setting, 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 (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- We recognise that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

- We recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, we 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 PSHE and SRE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between pupils.

9.2 Youth Produced Sexual Imagery ("Sexting")

- Lamberhurst St Mary's 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 UKCCIS guidance: 'Sexting in schools and 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.
- 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 youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using the school's provided or personal equipment.
- We will not:
    - View any suspected youth produced sexual imagery, unless there is no other possible option, or there is a clear safeguarding need or reason to do so.
        - If it is deemed necessary, the image will only be viewed by the 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 pupils to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
    - act in accordance with our child protection policy 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 pupils personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice. If an 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.
    - carry out a risk assessment in line with the UKCIS and KSCMP guidance which considers the age and vulnerability of pupils involved, including the possibility of carrying out relevant checks with other agencies.

- inform parents and 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 pupils, 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; the leadership team will also review and update any management procedures, where necessary.

9.3 Online Child Sexual Abuse and Exploitation (including child sexual abuse and sexual or criminal 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.
- The school 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.
- The school 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 CEOP
- 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.

9.4 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 to the age and ability.
- 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.
    - 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 .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - 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.

9.5 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.

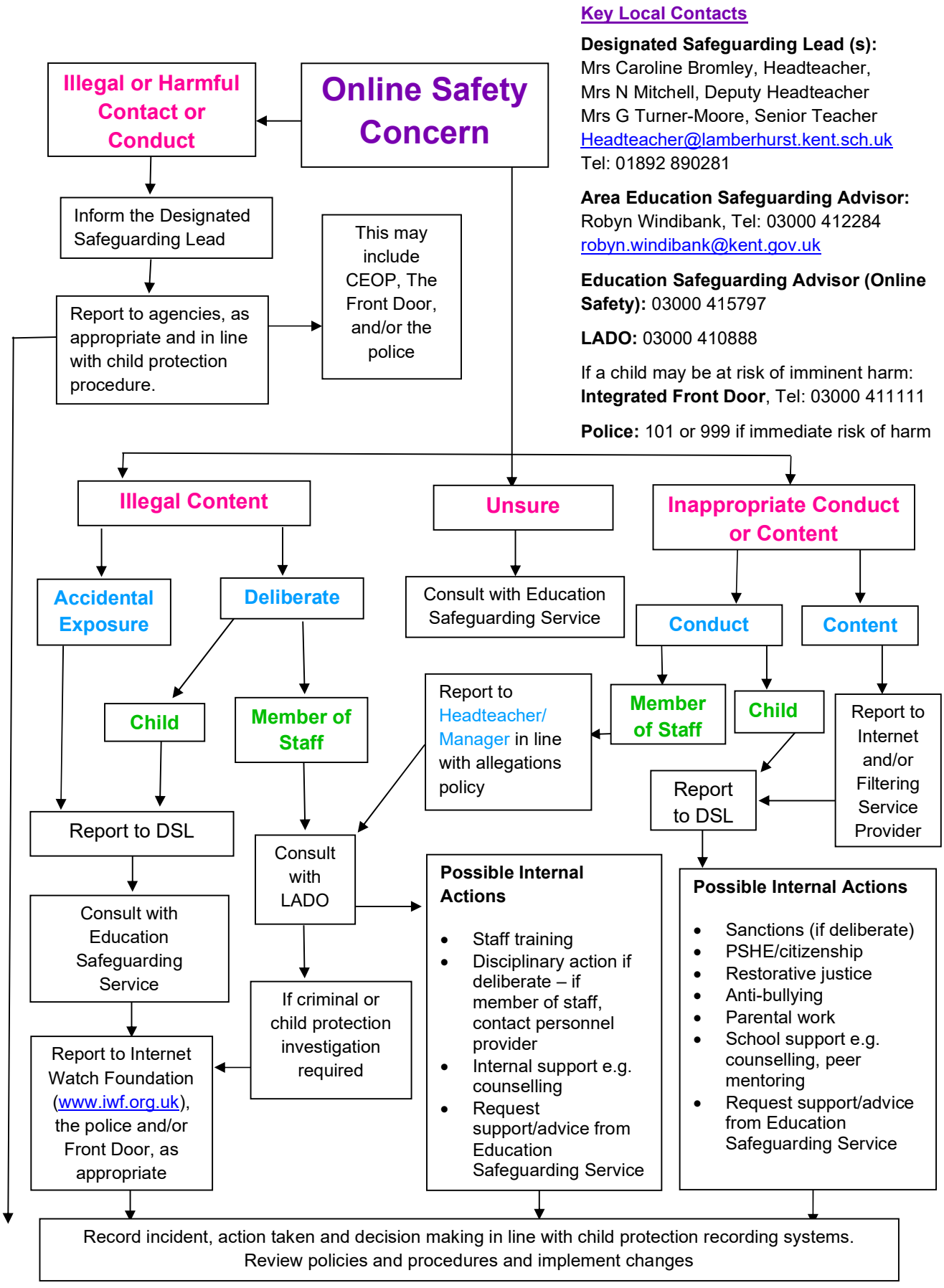
9.6 Online Hate

- 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.

9.7 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.

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

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:

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

Other:

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

National Links and Resources for Schools, Pupils and Parents/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