Online Safety Policy

Reviewed: **September 2024**

Reviewed by: **Headteacher / SLT / Governors**

Date to be reviewed: **September 2025**

***East Peckham Primary School**, 130, Pound Road, East Peckham, Tonbridge, TN12 5LH*

Designated Safeguarding Leads:
Kate Elliott - Headteacher, Bradley Atkins - Deputy Headteacher, Ellie Ray - Business Manager, Sarah Sinden - EYFS/KS1 Leader, Kate Worrall - SENCo

Named Governor with Lead Responsibility:
Stephen Hollands

Contents

1. Policy Aims

This online safety policy has been written by East Peckham Primary involving staff, learners and parents/carers, building on the Kent County Council/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' 2024, Early Years and Foundation Stage 2017,'Working Together to Safeguard Children' 2018 and the Kent Safeguarding Children Board procedures.

· The purpose of East Peckham Primary online safety policy is to:

- Safeguard and protect all members of East Peckham Primary community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

· East Peckham Primary 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

- East Peckham Primary believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- East Peckham Primary identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- East Peckham Primary believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, 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 learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as work laptops, tablets or mobile phones.

Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use Policies (AUP) and the Code of conduct
- Behaviour for Learning policy
- Child protection policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data protection
- Social Media policy

3 Monitoring and Review

Technology in this area evolves and changes rapidly. East Peckham Primary will review this policy at least annually.

- The policy will also be revised following any national or local policy requirements, any child protection concerns 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 or Deputy 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 practice and incidents, including outcomes.

Any issues identified via monitoring will be incorporated into our action planning.

4 Roles and Responsibilities

The Designated Safeguarding Leads (DSLs) have lead responsibility for online safety. East Peckham Primary recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct and acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Leads (DSLs) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside any deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented. Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- 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 learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- 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 settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet termly 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 online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and 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 settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

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

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the leadership team to ensure that the settings 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 is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

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

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

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

- Contribute to the development of the online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

· The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and Computing programmes of study
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

· The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology.
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

East Peckham Primary recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

East Peckham Primary will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

When implementing an appropriate online safety policy and curriculum East Peckham Primary will seek input from specialist staff as appropriate, including the SENCO.

5.3 Training and engagement with staff

We will:

· Provide and discuss the online safety policy and procedures with all members of staff as part of induction.

- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will be part of existing safeguarding and child protection training/updates
- This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.

· Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.

· Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.

· Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.

· Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.

· Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

· East Peckham Primary recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

· We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.
  - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

The information below is a duplicate of Section 6 of the 'Child Protection Policy'. In case of possible duplication error, the information in the Child Protection Policy is always to be the advice followed. Any information beyond the duplicated information (as indicated in the text), is available only in this policy.

6. Online Safety

- It is essential that children are safeguarded from potentially harmful and inappropriate material or behaviours online. East Peckham Primary will adopt a whole school approach to online safety which will empower, protect, and educate our pupils and staff in their use of technology, and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.

- East Peckham Primary will ensure online safety is considered as a running and interrelated theme when devising and implementing our policies and procedures, and when planning our curriculum, staff training, the role and responsibilities of the DSL and parental engagement.

- East Peckham Primary identifies that the 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 (including 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.

- East Peckham Primary recognises that technology, and the risks and harms related to it, evolve and change rapidly. The school will carry out an annual review of our approaches to online safety, supported by an annual risk assessment, which considers and reflects the current risks our children face online.

- The headteacher will be informed of any online safety concerns by the DSL, 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.

6.1 Policies and procedures

- The DSL has overall responsibility for online safety within the school but will liaise with other members of staff, for example IT leads and curriculum leads as necessary.

- The DSL will respond to online safety concerns in line with our child protection and other associated policies, including our Anti-bullying policy, Social Media policy and behaviour policies.
    - Internal sanctions and/or support will be implemented as appropriate.
    - Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.

- East Peckham Primary uses a wide range of technology. This includes: computers, laptops, tablets and other digital devices, the internet, our learning platform, intranet and email systems.
    - All school owned devices and systems will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

- East Peckham Primary recognises the specific risks that can be posed by mobile and smart technology, including mobile/smart phones, cameras and wearable technology. In accordance with KCSIE 2023 and EYFS 2021 East Peckham Primary has appropriate mobile and smart technology and image use policies in place, which are shared and understood by all members of the community.

6.2 Appropriate filtering and monitoring

- East Peckham Primary will do all we reasonably can to limit children's exposure to online harms through school provided devices and networks and in line with the requirements of the Prevent Duty and KCSIE, we will ensure that appropriate filtering and monitoring systems are in place.
- When implementing appropriate filtering and monitoring, East Peckham Primary will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.
- Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach to online safety and we recognise that we cannot rely on filtering and monitoring alone to safeguard our pupils; effective safeguarding practice, robust policies, appropriate classroom/behaviour management and regular education/training about safe and responsible use is essential and expected.
- Pupils will use appropriate search tools, apps and online resources as identified by staff, following an informed risk assessment.
- Internet use will be supervised by staff as appropriate to pupils age, ability and potential risk of harm.

Responsibilities

- Our governing body has overall strategic responsibility for our filtering and monitoring approaches, including ensuring that our filtering and monitoring systems are regularly reviewed, and that the leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
- Bradley Atkins, a member of the senior leadership team and Stephen Hollands, governor, are responsible for ensuring that our school/college has met the DfE Filtering and monitoring standards for schools and colleges.
- Our senior leadership team are responsible for
    - procuring filtering and monitoring systems.
    - documenting decisions on what is blocked or allowed and why.
    - reviewing the effectiveness of our provision.
    - overseeing reports.
    - ensuring that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.
    - ensuring the DSL and IT service providers/staff have sufficient time and support to manage their filtering and monitoring responsibilities.

- The DSL has lead responsibility for overseeing and acting on:
    - any filtering and monitoring reports.
    - any child protection or safeguarding concerns identified.
    - checks to filtering and monitoring system.
- The IT service providers/staff have technical responsibility for:
    - maintaining filtering and monitoring systems.
    - providing filtering and monitoring reports.

- completing technical actions identified following any concerns or checks to systems.
- working with the senior leadership team and DSL to procure systems, identify risks, carry out reviews and carry out checks.

- All members of staff are provided with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of our induction process, and in our child protection staff training.

- All staff, pupils and parents/carers have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

Decision making and reviewing our filtering and monitoring provision

- When procuring and/or making decisions about our filtering and monitoring provision, our senior leadership team works closely with the DSL and the IT service providers/staff. Decisions have been recorded and informed by an approach which ensures our systems meet our school specific needs and circumstances, including but not limited to our pupil risk profile and specific technology use.
- Any changes to the filtering and monitoring approaches will be assessed by staff with safeguarding, educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- Our school undertakes an at least annual review of our filtering and monitoring systems to ensure we understand the changing needs and potential risks posed to our community.

Appropriate filtering

- **The school's broadband provider, E2BN, provides web filtering tailored to our school needs. The web filtering meets the** DfE Filtering and monitoring standards for schools and colleges.
- Procedures / processes in place:
    - Our broadband has a firewall to prevent unauthorised access to our network
    - URL and Content web filtering (fully DfE compliant) to ensure pupils and staff safe when they are online
    - Two-factor login to cloud based platform to provide secure access between remote sites and for home access working
    - If learners or staff discover unsuitable sites or material, they are required to: turn off the screen and notify an adult immediately. The adult then notifies the DSL's and they respond by checking the website before contacting the IT Service to deal with the incident as required.
    - All users will be informed that use of our systems can be monitored, and that monitoring will be in line with data protection, human rights, and privacy legislation.
    - Filtering breaches or concerns identified through our monitoring approaches will be recorded and reported to a DSL who will respond as appropriate.
    - Any access to material believed to be illegal will be reported immediately to the relevant agencies, such as the Internet Watch Foundation and the police.

- East Peckham Primary School's education broadband connectivity is provided through E2BN and uses Protex Web Filtering provided by E2BN.
- E2BN is a member of Internet Watch Foundation (IWF).
- E2BN has signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- E2BN is blocking access to illegal content including child sexual abuse material (CSAM).

- E2BNblocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.

- We filter internet use on all school owned, or provided, internet enabled devices and networks. This i

- Our filtering system is operational, up to date and is applied to all users, including guest accounts, all school owned devices and networks, and all devices using the school broadband connection.

- We work with E2BN and our IT service providers to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.

- If there is failure in the software or abuse of the system, for example if pupils/students or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to:
    - Turn off the screen/ put the screen down and report to an adult in the room
    - The adult removes the device and reports it to the lead DSL and IT Lead Bradley Atkins
    - The lead DSL and IT Lead will liaise with E2BN if needed to block URL or rectify the issue

- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our child protection, acceptable use, allegations against staff and behaviour policies.

- Parents/carers will be informed of filtering breaches involving their child.

- Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material), Kent Police, NCA-CEOP or Kent Integrated Children's Services.

- If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or leadership team.

Appropriate monitoring

We will appropriately monitor internet use on all school provided devices and networks. This is achieved by:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software (SENSO)
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

- All users will be informed that use of our devices and networks can/will be monitored and that all monitoring is in line with data protection, human rights and privacy legislation.
- If a concern is identified via our monitoring approaches:
    - Where the concern relates to pupils/students, 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 policies.
    - Where the concern relates to staff, it will be reported to the headteacher (or chair of governors if the concern relates to the headteacher), in line with our staff behavior/ allegations policy.

- Where our monitoring approaches detect any immediate risk of harm or illegal activity, this will be reported as soon as possible to the appropriate agencies; including but not limited to, the emergency services via 999, Kent Police via 101, NCA-CEOP , LADO or Kent Integrated Children's Services.

6.3 Remote/Online learning

- East Peckham Primary will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements and any local/national guidance.

- All communication with pupils and parents/carers will take place using school provided or approved communication channels; for example, school office email accounts and phone numbers and/or agreed systems, via Google Classroom and Arbor.
    - 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 school 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).

6.4 Online Safety Training for Staff

- East Peckham Primary will ensure that all staff receive online safety training, which, amongst other things, will include providing them with an understanding of the expectations, applicable roles and their responsibilities in relation to filtering and monitoring, as part of induction.

- Ongoing online safety training and updates for all staff will be integrated, aligned and considered as part of our overarching safeguarding approach.

6.5 Educating pupils

- East Peckham Primary will ensure a comprehensive whole school curriculum response is in place to enable all pupils to learn about and manage online risks effectively as part of providing a broad and balanced curriculum. See section 9 for more information.

6.6 Working with parents/carers

- East Peckham Primary will build a partnership approach to online safety and will support parents/carers to become aware and alert of the potential benefits and risks and to reinforce the importance of children being safe online by:

- Providing information on our school website and through existing communication channels (such as official social media, newsletters),
- offering specific online safety events for parents/carers,
- or highlighting online safety at existing events.

- East Peckham Primary will ensure parents and carers understand what systems are used to filter and monitor their children's online use at school, what their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child is going to be interacting with online.

Where the school is made aware of any potentially harmful risks, challenges and/or hoaxes circulating online, national or locally, we will respond in line with the DfE 'Harmful online challenges and online hoaxes' guidance to ensure we adopt a proportional and helpful response.

The information below is only available in this policy and is no longer a duplicate of the content in the Child Protection Policy.

7. Safer Use of Technology

7.1 Classroom Use

East Peckham Primary uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Digital cameras, webcams and video cameras

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.

Supervision of learners will be appropriate to their age and ability.

Early Years Foundation Stage and Key Stage 1

- Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

Key Stage 2

- Learners will use age-appropriate search engines and online tools.
- Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.
- Google CLassroom will be deployed to facilitate children's learning
- Device will be monitored in 'real-time' using the SENSO software

7.2 Managing Internet Access

We will maintain a digital record of users who are granted access to our devices and systems. All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

7.3 Filtering and Monitoring

This is managed by E2BN, the schools broadband provider and Levett Consultancy, the schools IT management support.

Google workspace is used to manage the East Peckham domain and has inbuilt adjustable controls to support online safety for all devices connected to the East Peckham broadband network.

7.3.1 Decision Making

East Peckham Primary governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.

The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.

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.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

Education broadband connectivity is provided through E2BN.

E2BN block sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.

The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

We work with E2BN to ensure that our filtering policy is continually reviewed.

· If learners discover unsuitable sites, they will be required to:

- Turn off monitor/screen and report the concern immediately to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to one of the DSLs and technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.

Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

7.3.4 Monitoring

We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:

- physical monitoring (supervision),
- monitoring internet and web access (SENSO)

If a concern is identified via monitoring approaches one of the DSLs *will respond in line with the child protection policy.*

All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

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

7.5 Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.

- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network. Specific user logins and passwords will be enforced for all users.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found in the Acceptable Use Policy.

7.5.1 Password policy

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

All learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.

We require all users to:

- Use strong passwords for access into our system.
- Change their passwords regularly
- 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.

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 learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.

The administrator account for our website will be secured with an appropriately strong password and we will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

7.8 Managing Email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use 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.
- Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

Members of the community will immediately tell one of the DSLs if they receive offensive communication, and this will be recorded in our safeguarding files/records.

Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts will be blocked on site.

7.8.1 Staff email

The use of personal email addresses by staff for any official setting business is not permitted. All members of staff are provided with an email address to use for all official communication.

Members of staff are encouraged to have an appropriate work life balance when responding to email.

All emails to/from parents will go via the office email address. No member of staff should email parents direct unless permission is given by the Headteacher.

7.8.2 Learner email

·Learners do not have access to email

7.9 Management of Learning Platforms

East Peckham Primary uses Google Workspace as its official learning platform. Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
Only current members of staff and governors will have access to the LP.
When staff or governors leave the setting, their account will be disabled or transferred to their new establishment.

Staff and governors will be advised about acceptable conduct and use when using the LP.

All users will be mindful of copyright and will only upload appropriate content onto the LP.

Any concerns about content on the LP will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement.
  - A learner's parents/carers may be informed.
- If the content is illegal, we will respond in line with existing child protection procedures.

Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.

A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

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

We use Tapestry in Early Years to track learners progress and share appropriate information with parents and carers.

The Headteacher or Deputy Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard learner's data:

- Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps

which record and store learners' personal details, attainment or images.

- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

Please refer to our Social Media Policy.

9. Use of Personal Devices and Mobile Phones

East Peckham Primary recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

9.1 Expectations

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.

Electronic devices of any kind that are brought onto site are the responsibility of the user.

- All members of East Peckham Primary community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- All members of East Peckham Primary community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, toilets and swimming pools.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.

All members of East Peckham Primary community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place (e.g. staffroom) during lesson time.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Not use personal devices during teaching periods, unless written permission has been given by the headteacher, such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.

- Any pre-existing relationships, which could undermine this, will be discussed with the headteacher.

Staff will not use personal devices:

- To take photos or videos of learners and will only use work-provided equipment for this purpose.
- Directly with learners and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy

- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Learners Use of Personal Devices and Mobile Phones

Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

East Peckham Primary does not allow learners' personal devices or mobile phones to be brought in to school. The only exception to this is learners in year 6 who may require a phone if walking to and from school alone. In this case phones must be switched off and handed to the headteacher/deputy headteacher on the gate in the morning.

- Some exceptions are made for Year 5 children on the Headteacher's authority.

If a learner needs to contact his/her parents or carers they will be allowed to use the phone in the school office.

If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the headteacher.

If a learner breaches the policy, the phone or device will be confiscated and will be by the headteacher/deputy headteacher.

- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Searches of mobile phone or personal devices will only be carried out in accordance with our policy.
- Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
- Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including volunteers and contractors) should ensure that mobile phones are switched off, or left in the school office.

We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

Visitors (including volunteers and contractors) who are on site for a regular or extended period will use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSLs (or deputy) of any breaches our policy.

9.5 Officially provided mobile phones and devices

Members of staff may be issued with a work phone number and email address, where contact with learners or parents/ carers is required.

Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be

accessed or used by members of staff.
Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

10. Responding to Online Safety Incidents and Concerns

All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.

- Learners, 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 learners 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 Service.
Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Service or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the headteacher or deputy headteacher will speak with Kent Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

10.1 Concerns about Learners Welfare

The DSLs will be informed of any online safety incidents involving safeguarding or child protection concerns. These will be recorded on CPOMS..
The DSLs will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

Any complaint about staff misuse will be referred to the headteacher in accordance with the allegations policy. · Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.
East Peckham Primary 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, unwanted sexual comments and messages on social media, and online sexual exploitation.

- Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

East Peckham Primary recognises 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.

East Peckham Primary also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

East Peckham Primary will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

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 DSLs and act in accordance with our child protection and anti-bullying policies.
- If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSLs 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.

11.2 Youth Produced Sexual Imagery ("Sexting")

East Peckham Primary recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSLs.

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 KSCB guidance: "Responding to youth produced sexual imagery".

East Peckham Primary will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took

place on site or using setting provided or personal equipment.

We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- If it is deemed necessary, the image will only be viewed by the DSLs (and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
- Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

East Peckham Primary will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

East Peckham Primary recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSLs.

We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.

- If appropriate, store any devices involved securely.
- Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

If we are unclear whether a criminal offence has been committed, the DSLs will obtain advice immediately through the Education Safeguarding Service and/or Kent Police.

If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL (or deputy).

If learners at other setting are believed to have been targeted, the DSLs will seek support from Kent Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

East Peckham Primary will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSLs will obtain advice immediately through Kent 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), Kent police.

If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSLs are informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that one of the DSLs are informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet

Watch Foundation via www.iwf.org.uk .

- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the Headteacher or Deputy Headteacher is informed in line with our managing allegations against staff policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at East Peckham Primary .

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

11.6 Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated at East Peckham Primary and will be responded to in line with existing policies, including anti-bullying and behaviour.
All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
The Police will be contacted if a criminal offence is suspected.
If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Service and/or Kent Police.

11.7 Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSLs 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 or Deputy Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

12. Useful Links for Educational Settings

Kent Support and Guidance for Educational Settings

Education Safeguarding Service:

· Rebecca Avery, Education Safeguarding Advisor (Online Protection)
· Ashley Assiter, Online Safety Development Officer

o Tel: 03000 415797

· Guidance for Educational Settings:

www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding

www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials

www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links

www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCB:

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

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 Educational Settings

· CEOP:

www.thinkuknow.co.uk

www.ceop.police.uk

· Childnet: www.childnet.com

· Internet Matters: www.internetmatters.org

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

· Lucy Faithfull Foundation: www.lucyfaithfull.org

· NSPCC: www.nspcc.org.uk/onlinesafety

o ChildLine: www.childline.org.uk

o Net Aware: www.net-aware.org.uk

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

· UK Safer Internet Centre: www.saferinternet.org.uk

o Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

· 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

· Action Fraud: www.actionfraud.police.uk

· CEOP:

o www.thinkuknow.co.uk

o www.ceop.police.uk

· Childnet: www.childnet.com

· Get Safe Online: www.getsafeonline.org

· Internet Matters: www.internetmatters.org

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

· Lucy Faithfull Foundation: www.lucyfaithfull.org

· NSPCC: www.nspcc.org.uk/onlinesafety

o ChildLine: www.childline.org.uk

o Net Aware: www.net-aware.org.uk

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

UK Safer Internet Centre: www.saferinternet.org.uk