

Easthampstead Park Community School Online Safety Policy



Policy Aims

This online safety policy has been written by Easthampstead Park Community School. It takes into account the DfE statutory guidance "[Keeping Children Safe in Education](#)" 2018.

The purpose of the Easthampstead Park Community School online safety policy is to:

- Safeguard and protect all members of Easthampstead Park Community School 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.

Easthampstead Park Community 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.

Roles and Responsibilities

The school has appointed Mrs Liz Cook as Designated Safeguarding Lead (with Ms Charlotte Osborn as Child Protection Officer) to be the online safety lead.

Easthampstead Park Community School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

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 Code of conduct, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- 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.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.

- 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.

The Designated Safeguarding Lead (DSL) 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. Ms A Evans (Online Safety Lead) will be made aware of Child Protection issues arising from online safety.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- 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 schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.

It is the responsibility of all members of staff to:

- Read and adhere to the online safety policy.
- Take responsibility for the security of school 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 school's safeguarding policies and procedures, logging concerns on CPOMS and through Easthampstead IT Support.
- 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.

It is the responsibility of staff managing the technical environment (Tri-Computers) 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 to ensure that the school's IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

- Ensure that the school's filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.

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

- Engage in age appropriate online safety education opportunities.
- 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.

It is the responsibility of parents and carers to:

- Understand the school's expectations regarding e-safety and safe online activity, and encourage their children to adhere to them.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

Education and Engagement Approaches

Training and engagement with students

The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Discovery School IT lessons, covering use both at school and home.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The school will support pupils 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.
- Providing online safety education and training as part of the transition programme across the key stages.
- Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.

Easthampstead Park Community School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. Easthampstead Park Community School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.

Training and engagement with staff

The school will:

- Provide and discuss the online safety policy with all members of staff as part of their induction on joining EPCS.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. This will take place as part of existing safeguarding and child protection training/updates or within separate or specific online safety sessions in school staff meetings.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

Awareness and engagement with parents and carers

Easthampstead Park Community School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.

The school will build a partnership approach to online safety with parents and carers by:

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

Reducing Online Risks

Easthampstead Park Community 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 users can only access appropriate material. This is provided by Cyberoam and managed by TriComputers.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.

Safer Use of Technology

Classroom Use

- Easthampstead Park Community School uses a wide range of technology. This includes access to:
 - Computers, laptops and other digital devices
 - Internet which may include search engines and educational websites
 - School learning platform/intranet (Google Suite)
 - Email
 - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's Acceptable Usage Policy and with appropriate safety and security measures in place. The tablets have school-specific image and are monitored through Kaseya (anti-virus agent). Devices can be remotely controlled as appropriate.
- Students will be taught appropriate search techniques.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.

Managing Internet Access

The school will maintain a written record of users who are granted access to the school's devices and systems. All staff, pupils and visitors will read and sign an Acceptable Usage Policy before being given access to the school computer system, IT resources or internet.

Filtering and Monitoring

- The school uses educational broadband connectivity through BT.
- The school uses Cyberoam 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.
- The school works with TriComputers and Cyberoam to ensure that our filtering policy is continually reviewed.
- The school will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved through the use of AB Tutor by staff will be used to monitor classroom internet and web access

The school has a clear procedure for reporting filtering breaches.

- If pupils discover unsuitable sites, they will be required to inform their teacher immediately, turn off their screen if appropriate.
- The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or the IT Help desk via the ticketing system.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.

- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: Thames Valley Police and/or CEOP.

Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation. Full information can be found in the data protection policy, confidentiality policy and privacy policy.

Security and Management of Information Systems

The school takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- 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.
- Regularly checking files held on the school's network,
- The appropriate use of user logins and passwords to access the school network.
- Specific user logins and passwords will be enforced for all.
- All users are expected to log off or lock their screens/devices if systems are unattended.

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 7, all pupils are provided with their own unique username and private passwords to access school systems; pupils are responsible for keeping their password private.
- We require all users to:
 - Use strong passwords for access into our system.
 - Change their passwords when advised.
 - 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.

Managing the Safety of the School Website

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

Publishing Images and Videos Online

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

Managing Email

Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of conduct.

- The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell the DSL if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- The school has a dedicated system (CPOMS) for reporting child protection, wellbeing and pastoral concerns.

Staff Email:

- All members of staff are provided with a specific school 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 and pupils and parents.

Student Email:

- Pupils will use school provided email accounts for educational purposes.
- Pupils will sign 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 through the use of school email or Google Classroom.

Management of Learning Platforms

- Easthampstead Park Community School uses Google Suite as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Google Suite in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff, pupils and parents will have access to the Google Suite. When staff and/or pupils' leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Pupils and staff will be advised about acceptable conduct and use when using the Google Suite.

- All users will be mindful of copyright and will only upload appropriate content onto the Google Suite.
- Any concerns about content on the learning platform will be recorded and dealt with in the following ways:
 - The user will be asked to remove any material deemed to be inappropriate or offensive.
 - If the user does not comply, the material will be removed by the site administrator.
 - Access to the LP for the user may be suspended.
 - The user will need to discuss the issues with a member of leadership before reinstatement. e) A pupil's parent/carer may be informed.
 - If the content is considered to be illegal, then the school will respond in line with existing child protection procedures.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the learning platform by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

Social Media

Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Easthampstead Park Community School community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Easthampstead Park Community School community are expected to engage in social media in a positive, safe and responsible manner, at all times.
- All members of the Easthampstead Park Community School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Concerns regarding the online conduct of any member of Easthampstead Park Community School community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child protection policies.

Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the AUP.
- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites as strictly as they can.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of Easthampstead Park Community School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Deputy Headteacher immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

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

Students Use of Social Media

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

- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications and report concerns both within school and externally.

Official Use of Social Media

Easthampstead Park Community School has official media channels on Facebook, Twitter and Instagram. The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.

- The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
- Staff use school provided email addresses to register for and manage any official school social media channels.
- Official social media sites are suitably protected.
- Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Confidentiality and Child protection.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
 - Be professional at all times and aware that they are an ambassador for the school.
 - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
 - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
 - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
 - Ensure that they have appropriate written consent before posting images on the official social media channel.
 - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
 - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
 - Inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

Use of Personal Devices and Mobile Phones

Easthampstead Park Community School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but

technologies need to be used safely and appropriately within school. Please see Mobile Phone policy for further details.

Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Child protection and Image use.
- The school will ensure appropriate signage and information is displayed/ provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

Officially provided mobile phones and devices

- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the Acceptable use policy and other relevant policies.

Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
 - Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Local Safeguarding Children Board (LSCB) or Thames Valley Police (TVP) using 101 or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Thames Valley Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

Concerns about Pupils' Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
 - The DSL will record these issues in line with the school's child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Local Safeguarding Children Board thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

- Child Protection concerns will initially be logged by staff on CPOMS.

See Appendix A for details of procedures for responding to specific online incidents or concerns involving students.

Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, according to the Allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

Reviewed and Revised:	March 2020
Responsibility for implementation and review:	AHT with responsibility for e-safety Student Support Committee
Date of next review:	March 2021

Appendix A:

Procedures for Responding to Specific Online Incidents or Concerns

Youth Produced Sexual Imagery or “Sexting”

- Easthampstead Park Community School recognises youth produced sexual imagery (known as “sexting”) as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If the school are 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 and Safeguarding policies and the relevant Kent Safeguarding Child Board’s procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store the device securely.
 - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
 - Carry out a risk assessment which considers any vulnerability of pupil(s) 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 Specialist Children’s Services and/or the Police, as appropriate.
 - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
 - Implement appropriate sanctions in accordance with the school’s 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 school 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.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school 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. In this case, the image will only be viewed by the Designated Safeguarding Lead 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 children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

Online Child Sexual Abuse and Exploitation

- Easthampstead Park Community School 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.

- Easthampstead Park Community School recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally and include links to such organisations on its website.
- If the school are made aware of an incident involving online sexual abuse of a child, the school will:
 - Act in accordance with the school's Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store any devices involved securely.
 - Immediately inform Thames Valley 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.
 - Make a referral to Specialist Children's Services (if required/ appropriate).
 - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
 - Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
 - Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report :
www.ceop.police.uk/safety-centre/
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be referred to the MASH (Multi-Agency Safeguarding Hub) by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from Thames Valley Police and/or the LSCB first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- Easthampstead Park Community School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Thames Valley Police and/or the Education Safeguarding Team.
- If made aware of IIOC, the school will:
 - Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
 - Immediately notify the school Designated Safeguard Lead.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Thames Valley Police or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the school devices, the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
 - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
 - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
 - Ensure that the headteacher is informed.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
 - Quarantine any devices until police advice has been sought.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Easthampstead Park Community School
- Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy.

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Easthampstead Park Community School and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.

- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the LSCB or TVP.

Online Radicalisation and Extremism - Prevent

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school. Easthampstead Park School will monitor internet use through the AB Tutor and through the filtering system Cyberoam. Any concerns can be tracked through the filtering system as appropriate.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Child protection policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies.

Appendix B

Bracknell-Forest Support and Guidance

Bracknell Forest Local Safeguarding Children Board

Where to find advice on recognising and tackling child sexual exploitation:

<http://www.bracknell-forest.gov.uk/cse-leaflet.pdf>

Where to find advice if you are worried about a young person who might be in danger of radicalisation into extremist organisations:

- https://safe.met.police.uk/terrorist_or_extremist_activity/get_the_facts.html
- <http://parentinfo.org/article/preventing-violent-extremism-what-parents-can-do>
- <http://www.bflscb.org.uk/parents-and-carers/protecting-your-child/hate-crime-extremism-and-radicalisation>
- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
 - esafetyofficer@kent.gov.uk 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
- In an emergency (a life is in danger or a crime in progress) dial 999.

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- CEOP:
 - www.thinkuknow.co.uk
 - 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
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk UK Safer Internet Centre: www.saferinternet.org.uk
 - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk