West Heath School

Ashgrove Road Sevenoaks TN13 1SR
www.westheathschool.com

Online Safety Policy

This policy has been written for…	All staff and students at West Heath School
Copies of this policy may be obtained from…	• The School **web site -** http://www.westheathschool.com • It is available as a hard copy on request from the **school office** • Hard copies for reference are filed in the **staff room**
This policy links with the following policies	This policy should be read in conjunction with the Anti-Bullying, Child Protection and Peer on Peer policies and procedures.
Participants and consultees in the formulation of this policy were…	Vice Principal, Care and Safeguarding, Strategic Head KS2/3, Attachment Lead, DSL, Student Services Committee and the Trustees of the School. A representative group of students were invited to make comments and suggestions.
Edition, Review frequency and dates	This is edition 4.3 released November 2018 This policy will be reviewed annually. This policy was reviewed in conjunction with changes to Keeping Children safe in Education September 2018 It is due for review January 2019.
Relevant statutory guidance, circulars, legislation & other sources of information are…	Keeping Children Safe in Education – September 2018 (DfE)
The Lead Member of staff is	Strategic Head KS2/3, Attachment Lead, DSL

The Rationale and Purpose of this policy	West Heath School believes that online safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles. The school identifies that the internet and information communication technologies are an important part of everyday life, so students must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online. West Heath School has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions. West Heath School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.
Appendices	This policy has 3 appendices.
Copying	No school policy is ever written in isolation. Acknowledgement of sources of advice and significant influence in the development and recording of policies at West Heath School are noted on the front page. We request that any schools or organisations incorporating large sections of this policy without alteration should make similar appropriate acknowledgement.
Who will write and review the policy	The Policy will be the responsibility of the Head of Residential Care and Safeguarding however the school has a dedicated DSL member overseeing online safety. Our On-line Safety Policy has been written by the school, building on the Kent County Council (KCC) Online Safety Policy and government guidance. It has been agreed by the Senior Leadership Team, approved by Student Services Committee and ratified by the Board of Trustees.
Teaching and Learning **Appropriate and safe classroom use of the internet and any associated devises**	Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information. The school's internet access will be designed to enhance and extend education. Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students. All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential. Supervision of students will be appropriately supervised when using technology, according to their ability and understanding. In the school's residential provision the school will balance children's ability

to take part in age appropriate peer activities online with the need for the school to detect abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).

All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.

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

Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

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

The school will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.

Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

The school will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment.

Managing Information Services

Reducing online risks

West Heath School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.

The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and students from accessing unsuitable or illegal content. An external agency, Message Labs, manages the configuration of the filtering.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school/setting computer or device.

	The school will audit technology use to establish if the online safety policy is adequate and that the implementation of the policy is appropriate. Methods to identify, assess and minimise online risks will be reviewed regularly by the schools leadership team.
Managing email Managing the school website	Students may only use school provided email accounts for educational purposes. All members of staff are provided with a specific school email address to use for any official communication. The use of personal email addresses by staff for any official school business is not permitted. The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider. Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email. Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality. Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records. Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and students and parents. Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be. School email addresses and other official contact details will not be used for setting up personal social media accounts. The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE). The contact details on the website will be the school address, email and telephone number. Staff or students' personal information will not be published. The Principal will take overall editorial responsibility for online content

	published and will ensure that information is accurate and appropriate.
	The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright. Students work will be published with their permission or that of their parents/carers. The administrator account for the school website will be safeguarded with an appropriately strong password. The school will post information about safeguarding, including online safety, on the school website for members of the community.
Use of social media	Expectations regarding safe and responsible use of social media will apply to all members of West Heath School and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others. All members of West Heath School will be encouraged to engage in social media in a positive, safe and responsible manner at all times. Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the school community. All members of West Heath School 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. The school will control student and staff access to social media and social networking sites whilst on site and when using school provided devices and systems The use of social networking applications during school hours for personal use is not permitted to KS3 and KS4 students, however use by KS5 students is acceptable as communication via social media can be an intrinsic part of their personal development and communication whilst at college. Inappropriate or excessive use of social media during school/work hours or whilst using school/setting devices may result in disciplinary or legal action and/or removal of Internet facilities. Any concerns regarding the online conduct of any member of staff or student on social media sites should be reported to the senior leadership team (SLT) and will be managed in accordance with policies such as anti-

Students	bullying, allegations against staff, behaviour and safeguarding/child protection. Any breaches of the school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection. Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy. Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes. Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc. Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present. Students will be advised on appropriate security on social media sites and will be encouraged to use passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications. Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected. Parents/carers will be informed of any official social media use with students and written parental consent will be obtained, as required. Any official social media activity involving students will be moderated by the school where possible. The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts within school specifically for children under this age. Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.

Staff	Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites. If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school. Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school. Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared. Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws. Staff must ensure that any image posted on any official social media channel have appropriate written parental consent. Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school/setting unless they are authorised to do so. Staff using social media officially will inform their line manager, the Designated Safeguarding Lead of any concerns such as criticism or inappropriate content posted online. Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels. Staff using social media officially will sign the school social media Acceptable Use Policy.
How should personal data be protected	Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

Policy Decisions

The school will maintain a current record of all staff and student who are granted access to the school's electronic communications.

How will Internet access be authorised

All staff must read and sign the Acceptable Use Policy before using any school ICT resource.

Students will have supervised access to the internet as part of their study programme and during social times. Failure to follow usage guidance will result in access being reviewed.

How will risks be assessed

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.

The school will audit ICT use to establish if the online policy is adequate and that the implementation of the online policy is appropriate.

Responding to online incidents and concerns

All staff and students will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for students.

Staff and students will be informed about the procedure for reporting online safety concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.

The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded.

The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.

Complaints about Internet misuse will be dealt with under the School's complaints procedure.

Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure.

Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Students, parents and staff will be informed of the schools complaints procedure.

Staff will be informed of the complaints and whistle blowing procedure.

	All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns. All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community. The school will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate. The school will inform parents/carers of any incidents of concerns as and when required. After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguards Team or Kent Police via 101 or 999 if there is immediate danger or risk of harm. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police. If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team. If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools in Kent. Parents and children will need to work in partnership with the school to resolve issues.
Persons with particular responsibilities	The school has appointed Designated Safeguarding Leads as appropriate members of the leadership team and an online safety lead. The school has appointed the Designated Safeguarding Leads (as listed below) and Glen Campbell, a member of the Board of Trustees to take lead responsibility for online safety (e-Safe*ty).* DSLs: • James Nunns, Principal and Chief Executive Officer • Julie Goodyear, Vice Principal, Care and Safeguarding • Photini Bohacek, Strategic Head KS2/3, Attachment Lead • Julie Bellamy, Head of Induction • David Perridge, Strategic Head of Staff Development • Nick Oldham, Deputy Principal

Other Participants & Stakeholders	Students Staff
Monitoring & Evaluation	SLT Student Services Committee Trustees

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

West Heath School ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").

The school will implement preventative approaches via a range of age and ability appropriate educational approaches for students, staff and parents/carers.

West Heath School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.

The school will follow the guidance as set out in the non-statutory UKCCIS advice 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB "Responding to youth produced sexual imagery" guidance
If the school are made aware of incident involving creating youth produced sexual imagery 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 DSL.
- Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved.
- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
- Inform parents/carers about the incident and how it is being managed.

The school will not view an 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 these cases the image will only be viewed by the DSL.

The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.

If an indecent image has been taken or shared on the school/settings network or devices then the school will take action to block access to all users and isolate the image.

The school will take action regarding creating youth produced sexual imagery, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

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

Responding to concerns regarding Online Child Sexual Abuse and Exploitation

West Heath School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.

The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

West Heath School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the DSL.

If the school is unclear if a criminal offence has been committed then the DSL 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) then it will be passed through to the CSET team by the DSL.

If the school are made aware of incident involving online child sexual abuse of a child then 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 designated safeguarding lead.
- Store any devices involved securely.
- Immediately inform Kent police via 101 (using 999 if a child is at immediate risk)
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).

    - Put the necessary safeguards in place for student(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.

- The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.

- The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.

- If students at other schools are believed to have been targeted then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.

- The school will ensure that the Click CEOP report button is visible and available to pupils and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

Responding to concerns regarding Indecent Images of Children (IIOC)

West Heath School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.

The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.

If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

- If the school/setting is made aware of Indecent Images of Children (IIOC) then 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 DSL.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), Kent police via 101 (using 999 if a child is at

immediate risk) and/or the LADO (if there is an allegation against a member of staff).

- If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
    - Ensure that the DSL 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.
- If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:
    - Ensure that the DSL.
    - 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.
- If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will:
    - Ensure that the DSL is informed or another member of staff in accordance with the school whistleblowing procedure.
    - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Follow the appropriate school policies regarding conduct.

Responding to concerns regarding radicalisation and extremism online

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of students.

When concerns are noted by staff that a child may be at risk of radicalisation online then the DSL will be informed immediately and action will be taken in line with the safeguarding policy.

Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately via the Education Safeguarding Team and/or Kent Police.

Responding to concerns regarding cyberbullying

Cyberbullying, along with all other forms of bullying, of any member of West Heath School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

All incidents of online bullying reported will be recorded.

There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

Students, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.

The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Students, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.

Sanctions for those involved in online or cyberbullying may include:

- Those involved will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of students involved in online bullying will be informed.
- The Police will be contacted if a criminal offence is suspected.

Responding to concerns regarding online hate

Online hate at West Heath School will not be tolerated. Further details are set out in the school policies regarding anti-bullying and behaviour
All incidents of online hate reported to the school will be recorded.
All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

Appendix B

Use of Personal Devices and Mobile Phones

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

Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Students

Whilst the Trustees give permission for phones to be brought to the School, responsibility for the phone rests with the student and the School will take no financial responsibility for loss. The school bears no responsibility for lost or confiscated items. Parents are responsible for restricting access to age related consent on mobile devices

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy.
- Head phones must not be worn during lessons unless permission to do so has been given
- Students must not use personal devices such as mobile phones, tablets or cameras to take photos or videos of members of staff and other students.
- Students must not use phones or MP3 players to broadcast music.
- Student's personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during lessons and while moving between lessons.
- Mobile phones or personal devices will not be used by students during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If a student needs to contact his/her parents/carers they will be allowed to use a school phone.
- Parents/carers are advised that they should only contact their child during break-time (10.50-11.10am) or lunchtime (12.30-1.15)
- Students should protect their phone numbers by only giving them to trusted friends and family members.
- Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- Mobile phones and personal devices must not be taken into examinations. Students' found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place and returned at the end of the school day. If students dispute this, or offend persistently, parents/carers will be asked to collect the phone/device from reception. In the case of boarding students, care staff will be asked to retain the device in the boarding environment.

- School staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the schools behaviour or bullying policy or could contain youth produced sexual imagery (sexting). The phone or device may be searched by a member of the SLT with the consent of the student or parent/carer and content may be deleted or requested to be deleted, if appropriate. Searches of mobile phone or personal devices will only be carried out in accordance with the schools policy.
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

Staff

Staff should make themselves aware of the following KCC Guidance:

- Safer Practice with Technology Guidance

http://www.kelsi.org.uk/pupil_support_and_wellbeing/safety,_health_and_wellbeing/child_protection_safeguarding/e-safety.aspx

- Safety Strategy and Guidance

https://shareweb.kent.gov.uk/Documents/KSCB/Safer%20Practice%20with%20Technology.pdf

Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.

Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.

Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.

- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the SLT in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school/setting policy then disciplinary action will be taken.

- 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 then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school/settings allegations management policy.

Staff are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.

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

- School staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the schools behaviour or bullying policy or could contain youth produced sexual imagery (sexting). The phone or device may be searched by a member of the Leadership team with the consent of the student or parent/carer and content may be deleted or requested to be deleted, if appropriate. Searches of mobile phone or personal devices will only be carried out in accordance with the schools policy.
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

Visitors

Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's acceptable use policy.

Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.

Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL any breaches of use by visitors.

Appendix C

Online Safety (e-Safety) Contacts and References

Kent Support and Guidance

Kent County Councils Education Safeguards Team:
www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding

Kent Online Safety Support for Education Settings

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
- esafetyofficer@kent.gov.uk Tel: 03000 415797

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

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kent e–Safety Blog: www.kentesafety.wordpress.com

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

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.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

Know the Net: www.knowthenet.org.uk

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

NSPCC: www.nspcc.org.uk/onlinesafety

Parent Port: www.parentport.org.uk

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

The Marie Collins Foundation: http://www.mariecollinsfoundation.org.uk/

Think U Know: www.thinkuknow.co.uk

Virtual Global Taskforce: www.virtualglobaltaskforce.com

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

360 Safe Self-Review tool for schools: https://360safe.org.uk/

Online Compass (Self review tool for other settings):
http://www.onlinecompass.org.uk/