Hillcrest School

A Specialist Maths & Computing College and Sixth Form Centre

Internet Use and Online Safety Policy

Date Policy due to be reviewed: June 2019

Committee Responsible for Policy: Full Governing Body Committee

Section 1: Introduction

All schools must have regards to 'Keeping children safe in education' (September 2018) when carrying out their duties to safeguard and promote the welfare of children. At Hillcrest School staff, students, parents/carers and governors recognise that they exist in a world where technology is readily available to all. The school embraces the impact that such technology can have on a young person's social development, employability and technological competency. Nevertheless, Hillcrest School takes very seriously its responsibility for the 'Online Safety' of its community. We recognise that the abuse of technology, including malicious use of social media and the Internet, can have profound psychological and material consequences for victims of such abuse and therefore make every effort to ensure that safe use of technology is ensured within and outside of school.

Hillcrest School believes that the use of information and communication technologies (ICT) in school brings great benefits. New technologies have become integral to the lives of young people in today's society, both within schools and in their lives outside of school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. However, young people have an entitlement to safe internet access at all times and we recognise our duty to protect young people from different online risks ranging from the threat of sexual exploitation, to involvement in gang activities and indoctrination from forms of extremist organisations.

The statutory curriculum requires students to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill. Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable. It is important that schools, libraries and youth clubs, as well as parents, adopt strategies for the safe and responsible use of the Internet.

WHAT IS ONLINE SAFETY?

Online Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children, young people and parents/carers about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The Schools' Online Safety Policy has been written to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole, and is compliant with GDPR guidance introduced in May 2018.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Hillcrest School with respect to the use of IT-based technologies.

- Safeguard and protect the children and staff.

- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.

- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.

- Have clear structures to deal with online abuse such as online bullying (noting that these need to be cross referenced with other school policies).

- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:
CONTENT

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

CONTACT

- Grooming (sexual exploitation, radicalisation, extremism etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

CONDUCT

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Section 2: Use of the Internet is important

The rapid developments in electronic communications are having many effects on society.

- The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

Internet benefits for education

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between students world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- share teaching materials with students and parents via 'ShowMyHomework'.

How the Internet will enhance learning

- The school Internet access is designed expressly for student use and will include filtering for all staff and student accounts.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will learn to evaluate Internet content

- If staff or students discover unsuitable sites, the URL (web site address) and content must be reported to IT Support. This will then be forwarded to Link2ICT and the relevant website will be blocked.
- Staff should ensure that the use of Internet derived materials by themselves and by students complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

New technologies

- Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom.

- New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access.

- ICT teachers and support staff should keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies.

Section 3 - Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy, in-line with GDPR guidance introduced in May 2018.
- This will be carried out by the Governors /Sub Committee receiving regular information about online safety incidents and monitoring reports.
- The Chair of the Governing Body has taken on the wider role of Safeguarding Governor. Monitoring the effectiveness of the school's online safety, including the monitoring of online safety, student and staff violation logs and filtering provision, is an important aspect of this role.

- As outlined in 'Keeping Children Safe in Education' (September 2018) the Governing Body are aware of their responsibility to ensure the school uses appropriate filtering and monitoring systems to ensure students are safe on-line as part of the school's wider e-safety policy. However, the Governing Body are mindful that 'over-blocking' can lead to unreasonable restrictions on what children can be taught with regards to on-line teaching and safeguarding.

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Leader.

- The Headteacher and members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

- The Headteacher and Senior Leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role

- At Hillcrest School there is a policy and procedure for Safeguarding Supervision, designed by the DSL and includes online safety. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- Our Data Protection Manager is Sharron Johnson.

Online Safety Coordinator (Designated Safeguarding Leader):

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.

- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.

- Provides training and advice for staff.

- Liaises with school technical staff.

- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.

- Meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs.

ICT Operations Manager:

In accordance with GDPR guidance (May 2018), the ICT Operations Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack;

- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply;

- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed;

- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;

- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;

- that the use of the network / internet/ remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction;

- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices;

- they have read, understood and signed the Staff Acceptable Use Policy (AUP);

- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction;

- they report any breaches of data protection guidance to the Headteacher immediately;

- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems;

- online safety issues are embedded in all aspects of the curriculum and other activities;

- pupils understand and follow the Online Safety Policy and acceptable use policies;

- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices;

- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Students:

- are responsible for using the school digital technology systems in accordance with the Acceptable Use Agreement.

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers:

- Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

- The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature.

- Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events and access to parents' sections of the website

Section 4: Information Systems Security

Local Area Network (LAN)

- Users must take responsibility for their network use.
- All users will be issued with a specific user name and password.
- Passwords must not be made available to any other user.
- Servers must be located securely and physical access restricted.
- The server operating system must be current with all security updates installed.
- Virus protection for the whole network must be current.
- Access by wireless devices must be actively managed.

Wide Area Network

- All staff and volunteers are responsible for ensuring that any personal data is kept securely and is not disclosed to third parties without authority.
- Users must ensure that they either log off or lock the screen when leaving a computer unattended.
- Personal data sent over the internet or taken off site must be encrypted. All members of staff will be provided with an encrypted memory stick and only these devices should be used to store school data and information.
- All staff laptops will be encrypted.
- Under GDPR guidance (May 2018) organisations can be fined up to £20 million if data protection regulations are breached.
- Any non-school memory sticks used by staff must be encrypted if they wish to use the device on school machines. Data from non-school memory sticks should be transferred to new school provided encrypted memory sticks. It is a disciplinary offence for staff to use their own unencrypted memory sticks to store school data and information.
- Unapproved software will not be allowed in students' work areas or be attached to an email.
- Virus protection will be installed and updated regularly.
- Files on the school's network will be regularly checked. Any inappropriate material will be removed with further actions or sanctions taken as necessary.

Wireless Network

- All users have a requirement to maintain the security of the network and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Appropriate staff mobile devices will be given access to the Hillcrest wireless network only if they meet the network health check requirements. The connection details entered by the senior ICT technician. The password will remain confidential.

- When the students leave the school, the device will then be denied all access to the wireless network by MAC filtering.

Managing E-mail accounts and access

- E-mails should not be considered private and the school reserves the right to monitor all e-mail accounts.
- E-mails that contain confidential and sensitive information should be sent via an encrypted email or stored securely in the shared area.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Staff should endeavour to send one e-mail for each subject and not following on from another email conversation.
- Staff must only use school e-mail accounts to communicate with students and parents/carers.
- Staff should not reply to an e-mail from a student if it is sent from the student's personal e-mail account.
- Staff should not register or share School e-mail for personal online websites.
- Staff should be aware that e-mail activity is monitored by IT Network Support.
- Staff should keep their e-mail inbox up to date and regularly dispose of emails not required and keep those needed in separate folders.
- Access in school to external personal e-mail accounts will be blocked.

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher or IT Support if they receive offensive e-mail.
- Students must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Excessive social e-mail use can interfere with learning and may be restricted.
- The forwarding of chain letters, by staff and/or students, is not permitted.
- The forwarding of inappropriate messages, by staff and/or students, is not permitted.

Internet Access

The school's internet is filtered and monitored throughout the school day. Additional filters are available through monitoring software that have been purchased to ensure that students are making appropriate use of the internet. Internet access is granted to all staff and students on the basis of educational need. The filtering system is key to our role in safeguarding children from all potential online risks associated with child sexual exploitation, forced marriage, recruitment in gangs, people trafficking and radicalisation by extremist groups.

Managing Web site content

- The point of contact on the Web site will be the school address, school e-mail and telephone number.
- Staff or students' home information will not be published.

- Web site photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material will held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Managing Emerging Internet applications

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Internet access records

- By using the Internet, secondary students are agreeing to abide by the Responsible Internet Use statement.

- Parents will be asked to sign and return a form stating that they have read and understood the Acceptable Use Policy before the student is issued with their user name and password by IT Support.

- Staff and students will be asked to sign the Acceptable Use Policy at the start of each academic year.

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications (office group access has now be removed)

The risks will be assessed

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Access to Home Access Plus

- For staff and students with Internet access at home, it is possible for them to gain remote access to their school computer account in order to download / upload personal files. The uploading /downloading of files are subject to the same rules imposed whilst in school.

- All students will be provided with the means to access the school's network via HomeAcess Plus. Any violation of the terms, as set out below, governing remote access to the school's computer system, will result in remote access being withdrawn and may be considered, by law, to be a breach of the Computer Misuse Act (1990). Any violation of this agreement may result in the permanent removal of access outside of school. Any violations of a serious nature may result in the involvement of outside agencies (such as the Police), as directed by the Headteacher and School Governors.

- Use of this service is subject to the standard ICT Acceptable Use Policy and the completion of the Student Acceptable Use Agreement form, in addition to the following additional terms and conditions. The uploading of any files not directly related to schoolwork is strictly forbidden, as are files of the following nature:
    - Any virus infected files.
    - Executable files (e.g. computer software, self-extracting archives).
    - Command execution files (e.g. JAVA scripts, batch files).
    - Files containing any defamatory or unlawful text and/or images.
    - Encrypted and password protected files must have the key provided at the request of the Headteacher**.**

- Any computer used whilst accessing the school's computer system must have an approved and regularly updated anti-virus programme installed. User identity and passwords are to remain confidential at all times and must not be passed to any third party. All access to the system is monitored and audited; these logs will remain confidential unless requested by an authorised third-party.

- Users must not interfere with the correct operation of the system, access anyone else's account, or attempt to deny anyone else access to their account (denial of service) by any means.

Management of filtering

- The school will work in partnership with the LEA, DfES and the Internet Service Provider to ensure systems to protect students are reviewed and improved.

- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the ICT Operation Manager.

Section 5: Guidance for students

Social networking sites provide free, easy to use facilities. The school will control access to social media and social networking sites over the school network. Students will be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

- Students will be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile

or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs
- Students are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the student or his/her location.
- Students are advised on security and required to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.

Dissemination of rules and guidance to students

- Rules for Internet access will be posted in all rooms where computers are used.
- Students will be informed that Internet use will be monitored.
- Students will be asked to sign the Acceptable Use at the start of each academic year
- Instruction/reminder in responsible and safe use will precede Internet access.
- The rules regarding safe and acceptable use of ICT facilities is an integral part of the ICT and PSD curriculum. There is a yearly e-safety assembly.

Consequences for failure to follow Acceptable Use Policy

E-safety is an integral part of the school's 'Getting It Right' system. The school does not take responsibility for inappropriate use of digital media outside of school hours or outside of the school premises. Such issues which affect the running of the school will result in the involvement of any appropriate agency (e.g. the Police) and the school following the 'Getting it Right policy towards the individual. Under the GIR system the following consequences may be issued:

- Students using inappropriate websites in lessons will receive a C1
- Students downloading inappropriate material from the internet will receive a C3
- Students found sending inappropriate messages via the internet will receive a C4
- Recording any member of the school community without their permission is not allowed. The recording, displaying, supply or posting of any such materials will result in a **C5** exclusion. The school reserves the right to determine the length of any fixed term exclusions.

Safeguarding: Cyber-bullying

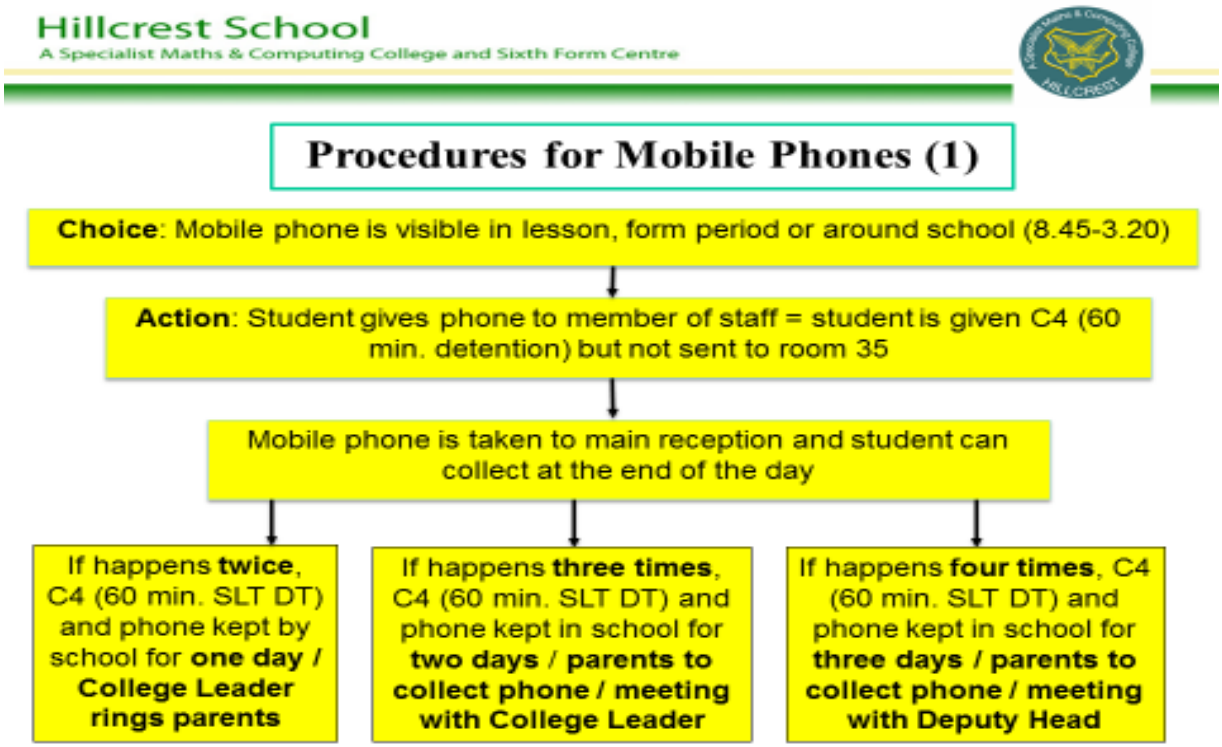
Cyber-bullying is defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007. It is essential that young people, school staff and parents and carers understand how cyber-bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users supports innovation and safety. Cyber-bullying will not be tolerated in school. Further details are set out in the Anti-Bullying Policy.

- All incidents of cyber bullying reported to the school will be recorded.

- All reported incidents or allegations of cyber bullying will be investigated:
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school reserves the right to involve any external agency deemed appropriate to resolve cyber-bullying issues on and out of school, ie – police, social care.

Personal Mobile devices (phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students and parents or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- If students bring a mobile phone or personally-owned device into school and are seen using the device ***anytime*** (including break times) during the school day the device will be confiscated and the student will receive a 60 minute after school detention.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from the classroom teacher.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- The Headteacher reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.



Safeguarding: Radicalisation

- We strongly recognize the risk posed to our students of on-line radicalization, as terrorist organizations like ISIL seek to radicalize young people through the use of social media and the internet. Research shows that ISIL propaganda includes images and videos that present the group as an exciting alternative to life in the West and that it uses its social media to encourage supporters to share the material with a wider online audience. ISIL promotes an image of success online in order to attract young people. The propaganda claims it is the duty of Muslin men and women in the West to join the fight against the West. The seriousness of the potential online threat is highlighted by the fact that 95,000 pieces of terrorist content has been removed from the internet since 2010.

- To combat this online threat, we use a system to filter and monitor student online behaviour on a daily basis. Trigger words, phrases and content is updated and reviewed on a regular basis.

- The Headteacher and DSL are notified of any inappropriate online behaviour and appropriate steps are taken as required. This may involve speaking to the student, contacting parents, setting up a mentoring programme or making a direct referral to the MASH team based on the seriousness of the incident. Our annual staff training ensures all staff are fully aware of the risks posed by the online activity of extremist and terrorist groups.

- E-safety is a key aspect of the school curriculum and equips pupils to stay safe online, both in school and outside. E-safety is delivered predominantly in the ICT curriculum with specific focus on the range of social media sites that could pose a threat to students. For example;

    - ISIL and EDL supporters use Facebook to share content, such as news stories and Youtube videos, among their peer groups. This is very common amongst far right extremist groups in the UK such as Combat 18, Young Patriots, Christian Patrol, Blood and Honour, National Action and Britain First.
    - Twitter is a popular platform for pro-ISIL and EDL accounts. It is easy to establish an account, stay relatively anonymous and share material.
    - Youtube is used to host videos, both with official ISIL output and videos created by users themselves. Multiple ‘dummy’ accounts will be set up so that when videos are taken down they can be reposted quickly.
    - ASK.FM is sometimes used by people considering traveling to Syria or Iraq and provides information on travel, living standards, recruitment fighting and broader ideology.
    - Instagram is used by fighters and ISIL supporters to share the photosets frequently used by ISIL media organisations.
    - Tumblr is an online blogging site and is used by ISIL fighters to promote longer, theological reasons why people should travel to Syria and Iraq. It is popular with female ISIL supporters, who have written blogs addressing the concerns girls have about traveling to the region, such as leaving their families and living standards in Syria.

- Private messaging apps, such as WhatsApp, Kik, SureSpot, Whisper, Yik Yak, Omegle and Viber, are also commonly used to share messages on what to pack to travel and who to contact when they arrive.

- E-safety is also delivered in other subjects, the PSD curriculum and in our whole school assembly programme. Our annual PSD audit identifies the extent of curriculum coverage for this and all other safeguarding themes.

E-Safety: CSE and Sexting

- Sexting is images or videos generated by children under the age of 18, or of children under the age of 18 that are of a sexual nature or are indecent. These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know.

- It is important to be aware that people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo images) of a person under 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to:

  - take an indecent photograph or allow an indecent photograph to be taken;
  - make an indecent photograph (this includes downloading or opening an image that has been sent via email);
  - distribute or show such an image;
  - possess with the intention of distributing images;
  - advertise; and possess such images.

<u>The extent of the issue</u>

- Over one third (38%) had received a sexually explicit text or email – 36% of males and 39% of females
- Over a quarter (25%) had received an offensive sexual image
- 85% knew the identity of the aggressor
- The majority were peers and only 2% indicated that it was an adult
- 6% had received a message or image on the subject of sex which subsequently made them feel uncomfortable or upset
- Over half of teachers (54%) were aware of pupils creating and sharing sexually explicit messages and images via the internet or mobile

<u>Steps to be taken in the event of a disclosure</u>

- If a student discloses about a potential sexting issue, the member of staff must consider if the student disclosing about themselves receiving an image, sending an image or sharing an image?
  - What sort of image is it? Is it potentially illegal or is it inappropriate?
  - Is it a school device or a personal device?
  - Does the student need immediate support and or protection?
  - Are there other students and or young people involved?
  - Do they know where the image has ended up?
  - How widely has the image been shared and is the device in their possession?

- Initial disclosure may be to a class teacher, non-teaching member of staff or peer. If this is the case;
  - Safeguarding / Child Protection Policy must be followed
  - Initial concern completed and reported immediately
  - All disclosures must be passed on to the DSL / Safeguarding Team
  - Clear record the incident should be made after referral to the DSL / Safeguarding Team
  - The Headteacher should be informed
  - There may be instances where the image needs to be viewed and this should be done in accordance with protocols.
  - Police should be informed of illegal activity

Searching a device

- A device can be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography. The revised Education Act 2011 gives schools the power to seize and search an electronic device if they think there is good reason for doing so. When searching a mobile device the following conditions apply:
  - The action is in accordance with the school's child protection and safeguarding policies
  - The search is conducted by the head teacher or a person authorised by them
  - A member of the safeguarding team is present
  - The search is conducted by a member of the same sex

Never …….

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the student/young person UNLESS there is clear evidence to suggest that there is an immediate problem
- Print out any material for evidence
- Move any material from one storage device to another

Always...

- Inform the school Designated Safeguarding Lead (DSL)
- Record the incident
- Act in accordance with school safeguarding and child protection policies and procedures
- Inform relevant Senior Leadership Team about the alleged incident before searching a device

If the image has been shared across a personal mobile device:

Always..

- Confiscate and secure the device(s)

Never...

- View the image unless there is a clear reason to do so
- Send, share or save the image anywhere
- Allow students to do any of the above

If the image has been shared across the school network, website or social network:

Always..

- Block the network to all users and isolate the image

Never...

- Send or print the image
- Move the material from one place to another
- View the image outside of the protocols in your safeguarding and child protection policies and procedures

If indecent images of a child are found the Safeguarding Team will;

- Store the device securely
- Carry out a risk assessment in relation to the young person
- Make a referral if needed
- Contact the police (if appropriate) it is not the responsibility of a school to make decisions about the seriousness of the matter
- Put the necessary safeguards in place for the student, e.g. they may need counselling support, immediate protection and parents must also be informed.
- Inform parents and/or carers about the incident and how it is being managed.

- We are aware that there may be a multitude of reasons why a student has engaged in sexting – it may be a romantic/sexual exploration scenario or it may be due to coercion. It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, as a school it is important that we record incidents are consistently. It may also be necessary to assist the young person in removing the image from a website or elsewhere.

- While any decision to charge individuals for such offences is a matter for the Crown Prosecution Service, it is unlikely to be considered in the public's interest to prosecute children. However, children need to be aware that they may be breaking the law. Although unlikely to be prosecuted, children and young people who send or possess images may be visited by police and on some occasions media equipment could be removed. This is more likely if they have distributed images. However, there are cases in which children and young people have been convicted and sent to prison. The important thing to remember is that whilst, as a school, we need to consider the implications of passing an incident over to the police, it is not the responsibility of the school to make decisions about the seriousness of the matter. Clearly, if it is a case that involves an adult, the process and potential outcome will be very different.

Containment and Student Reaction

- There are cases in which victims have had to leave or change schools because of the impact of the incident. As a school we will endeavour to provide necessary support for students.

    - Anxiety - who has seen the image and where it has ended up.
    - Reassurance - regarding its removal from the platform on which it was shared.
    - Support - from the school, their parents and their friends.
    - Observation - parents should usually be told what has happened so that they can keep a watchful eye over their child
    - Curriculum - reinforce to all students the impact and severe consequences that this behaviour can have.

Section 6: Guidance for Staff

Social Media

- All staff are made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They are made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

- Staff should not refer to Hillcrest school, other educational institutions, work related activities or make comments on national education policy on such sites that may bring the school or teaching profession into disrepute.

- Staff are discouraged from expressing political, religious, cultural or socio-economic views on any forms of social media as comments could be perceived as undermining the teaching profession.

- Staff should be aware that they are representing the school and profession at all times in the community and that other members of the community may know the school the member of staff works at even though it is not listed on their personal profile or referred to in comments made on different social media sites.

- Privacy settings should be high and updated regularly, ie – facebook accounts must be set at 'friends' level only.

- Staff must not post any images of other members of staff on such sites without their permission.

- Staff must not, under any circumstances, post images of students on such sites. In addition, staff are discouraged from posting images of their children, family or themselves involved in social activities that may undermine their role as a teacher, ie – posting images of themselves inebriated out of school.

- Staff are encouraged to remove personal images as profile pictures and ensure that their employment details, personal telephone numbers or email address are not recorded on personal details sections of any social media site.

- Staff must not engage in social network activity with current and previous students or parents under all circumstances.

Internet access and websites

- Any material accessed by staff that the school believes is illegal will be reported to appropriate agencies such as the Police. Accessing material considered inappropriate may result in the school initiating disciplinary actions against staff members as necessary.

- The school will regularly monitor staff internet activity on school lap equipment in and out of school. This monitoring will be carried out by a member of the Senior Leadership Team.

Use of school equipment

- Staff are issued with laptops on arrival at the school. The laptop is school property and should be explicitly used for appropriate school related business. The school,

however, recognises that occasional and appropriate personal use of the school's computers is beneficial both to the development of IT skills and for maintaining a positive work-life balance.

- During working hours staff must use school equipment for work-related activities only. It is prohibited to use school equipment at any time for inappropriate personal use. Among uses that are considered inappropriate are the following:

    - Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
    - Making ethnic, sexual preference, or gender related slurs or jokes

- Staff should be aware that any work uploaded to a laptop is automatically synced to the school servers.

- Staff should not attempt to bypass security or access restrictions in place on the computer system.

- Staff should ensure the all items of school portable computer equipment (such as laptops, cameras) are securely stored when taken off the school site or in a locked room or cupboard if left on the school site overnight or during school holidays.

Use of personal computers out of school

- Staff should ensure that any school-related sensitive or personal information, used on a personal computer at home or another device in the community (ie – public library), is secured to prohibit access by any non-member of staff, and encrypted to protect against theft.

Use of student images

- Images of a student must not be published without the parent's or carer's written permission. This permission is obtained when a student first joins the school.
- Staff should not use their own personal devices to take and store images of students. School cameras should always be used.

- All images of students should be stored on the school network and not on individual staff memory sticks. Staff should store all school-based photographs on the 'Photo Drive' on the shared staff area.

- All photographs will be deleted at the end of each academic year.

Data Protection

- Staff must be made aware of their responsibility to maintain confidentiality of school information.

- Staff are personally responsible and liable if they lose any school data, ie – theft of lap top or memory stick containing school data. Under GDPR guidance (May 2018) organisations can be fined up to £20 million if data protection regulations are breached.

- All staff and volunteers must immediately report any data breaches (ie – email sent to the wrong person, laptop and/or encrypted memory stick lost or stolen) to the Headteacher and the Data Protection Officer (Sharron Johnson). The school will then report the breach to the Information Commissioner's Office within 72 hours.

Mobile Phones / devices

- All mobile phones brought on site should be PIN protected in case of theft or loss. Staff must not use any form of personal devices to take and store photographs of students.

- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded.

- All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.

- The Headteacher reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

- Staff mobiles devices may be searched at any time as part of routine monitoring.

Student use of staff laptops

- Staff should not allow a student to have individual use of their account or access to their username / password information.

- Staff should not allow students to use their school lap top as students may gain access to confidential information or use the internet for inappropriate purposes.
- Staff should not leave their lap top unattended. It is essential that staff lock their computer if students are left unsupervised for a period of time.

Staff Files

- Staff should be aware that IT Network Support staff can access the content of all staff folders as necessary without permission from the individual member of staff.

Dissemination of rules for staff

- All staff are governed by the terms of the 'Responsible Internet Use' in school.

- All staff including teachers, supply staff, teaching assistants and support staff, will be provided with the School Internet and E-Safety Policy, and its importance explained.

- Staff should be aware that Internet traffic is filtered and traced to the individual user. Discretion and professional conduct is essential.

- The monitoring of Internet use is a sensitive matter and will be conducted by a member of the Senior Leadership Team.

- Staff development in safe and responsible Internet use and on the school Internet policy will be provided annually.

Complaints Procedure Regarding Internet Use

- Responsibility for handling incidents will be delegated to a senior member of staff.

- Any complaint about staff misuse must be referred to the Headteacher.

- Students and parents will be informed of the complaints procedure.

Section 7: Parental Support (see appendix 1)

- Parents' attention will be drawn to the School Internet and E-Safety Policy in newsletters, the school brochure and on the school Web site.

- The school will update the annual parent guide on e-safety and upload to the website. This is particularly relevant to the threat of online radicalisation by extremist ideologies. Information is provided for parents / carers on possible signs to suggest their child is at risk of becoming radicalised and parents / carers are signposted on the website to support organisations including THINKUKNOW, CHANNEL and FAST. The website also contains general information for parents / carers on how to keep their child safe from other online dangers included child sexual exploitation, involvement in gangs and people trafficking.

- Internet issues will be handled sensitively to inform parents without undue alarm.

- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

Section 8: Internet Use with in the school community

- Adult users will need to sign the acceptable use policy.

- Parents/carers of children under 16 years of age will be required to sign an acceptable use policy on behalf of the child.

- Visitors must agree to the code of conduct which is displayed during the user's logon to the network.

Section 9: Monitoring

Our Internet and Online Safety Policy has been written by the school. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

Name of responsible person: Steven Connor-Hemming

Date reviewed by SLT: June 2018

Date of next review: June 2019

Appendix 1

Online Safety guidance for parents

Almost all of our pupils use the Internet at home and we know that, as parents, it can be difficult to allow children the freedom to develop as responsible individuals while protecting them from the perils and pitfalls of the Internet. Increasingly, even at primary school age, younger people are conducting their social life online so parents need to provide guidance to make sure that their children behave safely and responsibly. Please help your children by following these key recommendations:

- **Talk regularly with your children about their use of technology and how they communicate with people online**
- **Keep computers and other web-enabled devices in family rooms**

CEOP top tips – **Tips for Parents**

As a parent you'll probably know how important the internet is to children and young people. They use it to learn, play, socialise and express themselves in all types of creative ways. This may be through sharing photos and videos, blogging, gaming, or even developing their own apps. It is a place of amazing opportunities.

The technology children use in their daily lives can seem daunting. You might worry about the risks they can face online, such as bullying, contact from strangers, as well as the possibility of access to inappropriate or illegal content. To help them stay safe, it's important that you understand how your child uses the internet.

By following this simple checklist, you can start to protect them and decrease the risks they face:

I have asked my child to show me sites they use - By doing so, your child is including you in their online life and social activity. Show an interest and take note of the names of their favourite sites. You can then re-visit these when you are alone. Take your time and explore the space, find out how to set the safety features and learn how to report any issues directly to the site.

I have asked my child to set their profile settings to private - Social networking sites, such as Facebook, are used by children to share information, photos and just about everything they do! Encourage your child to set their privacy settings to private. They need to think about the information they post online as it could be copied and pasted anywhere, without their permission. If it got into the wrong hands, somebody may wish to use it against them or worst of all try to locate them in the real world.

I **have asked my child about their online friends** - We know that people lie online about who they are and may create fake identities. It is very important children understand this. Whether they are visiting a social network or a gaming site, the safety messages are the same. Children and young people must never give out personal information and only be "friends" with people they know and trust in the real world.

I have set appropriate parental controls on my child's computer, mobile and games console - Filters on computers and mobiles can prevent your child from viewing inappropriate and possibly illegal content. You can activate and change levels depending on your child's age and abilities. You can also set time restrictions for using the internet or

games. They can be free and easy to install. Call your service provider who will be happy to assist or visit CEOP's parents' site for further information. Explain to your child why you are setting parental controls when you talk to them about their internet use.

My child has agreed to tell me if they are worried about something online - Sometimes children get into situations online where they don't feel comfortable or see something they don't want to see. By opening up the communication channels and talking to your child about the internet, their favourite sites and the risks they may encounter, they are more likely to turn to you if they are concerned about something.

I know where to get help if I'm concerned about my child - The CEOP Safety Centre provides access to a range of services. If you are concerned that an adult has made inappropriate contact with your child you can report this directly to CEOP. You can also find help if you think your child is being bullied, or if you've come across something on the internet which you think may be illegal.