



Policies

E-Safety Policy

Next review date: June 2029



Rationale

E-Safety encompasses the Internet and related electronic communications such as mobile phones and wireless technology. It highlights the need to educate our students about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Purpose

The purpose of Internet use at Holmes Chapel Comprehensive School and Sixth Form College (HCCS) 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 administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. The Governors and Headteacher at HCCS take seriously the responsibility to provide our students with high quality Internet access. The students will use the Internet outside school and, together with their parents, will need to learn how to evaluate Internet information and to take care of their own safety and security.

E-Safety Policy

An effective e-Safety policy is required to ensure that staff and students at HCCS are able to use the internet and related communications technologies appropriately and safely.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of Web filtering.
- National Education Network standards and specifications

1. Creating an e-Safety Ethos

1.1 Aims and policy scope

- HCCS believes that e-Safety is an essential element of safeguarding students and adults in the digital world, when using technology such as computers, mobile phones or games consoles.
- HCCS 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 so they can be empowered to build resilience online.
- HCCS has a duty to provide the school community with quality Internet access to raise education standards, promote student achievement, support professional work of staff and enhance the school's management functions. HCCS also identifies that with this there is a clear duty to ensure that students are protected from potential harm online.
- The purpose of HCCS's e-safety policy is to:
 - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that HCCS is a safe and secure environment.
 - Safeguard and protect all members of the HCCS community online.
 - Raise awareness with all members of the HCCS community regarding the potential risks as well as benefits of technology.
 - To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
 - Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on

behalf of the school (collectively referred to as 'staff' in this policy) as well as students and parents/carers.

- This policy applies to all access to the internet and use of information communication devices including personal devices or where students, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, AI Policy, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social Health and Education (PSHE), Citizenship and Sex and Relationships education (SRE).

1.2 Writing and reviewing the online safety policy

- HCCS's e-safety policy has been compiled by Neil Barnett (Strategic ICT Manager), building on the Kent County Council online safety policy template and The Key's model online safety policy.
- The policy has been approved and agreed by the Senior Leadership Team and governing body.
- The School has appointed a member of the Governing Body to take lead responsibility for e- Safety.
- The school has appointed a member of the leadership team as the e-safety lead.
- The schools e–Safety Policy and its implementation will be reviewed every 3 years.

1.3 Key responsibilities of the community

1.3.1 Key responsibilities of the Board of Governors are:

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

1.3.2 Key responsibilities of the HCCS leadership team are:

- Developing, owning and promoting the e-safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- Auditing and evaluating current e-safety practice to identify strengths and areas for improvement.
- Supporting the e-safety lead in the development of an e-safety culture within the school.
- Ensuring there are appropriate and up-to-date policies and procedures regarding e-safety.
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect students from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding e-safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that e-safety is embedded within a progressive whole school curriculum which enables all students to develop an age-appropriate understanding of e-safety and the associated risks and safe behaviours.
- Making appropriate resources available to support the development of an e-safety culture.
- Taking responsibility for e-safety incidents and liaising with external agencies as appropriate.
- Receiving and regularly reviewing e-safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the HCCS community to access regarding e-safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of school's systems and networks.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting e-safety.
- To ensure that the Designated Safeguarding Lead (DSL) works in partnership with the e-safety lead.

1.3.3 Key responsibilities of the designated safeguarding/e-safety lead are:

- Acting as a named point of contact on all e-safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that e-safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the HCCS lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an e-safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitor HCCS e-safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school leadership team, Governing Body and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating e-safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that e-safety is integrated with other appropriate school policies and procedures.

1.3.4 Key responsibilities of staff, trainees and volunteers are:

- Contributing to the development of e-safety policies.
- Reading the school Acceptable Use Policy (AUP) and adhering to it.
- Taking responsibility for the security of HCCS systems and data.
- Having an awareness of e-safety issues, and how they relate to the students in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding e-safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead.
- Knowing when and how to escalate e-safety issues, internally and externally.
- Being able to signpost to appropriate support available for e-safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.

1.3.5 Additional responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership team.
- To ensure that suitable access controls are implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the e-safety lead and DSL.
- Ensuring that the use of HCCS's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the e-safety lead and DSL.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the e Safety Incident Log, and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the e-safety lead and leadership team, especially in the development and implementation of appropriate e-safety policies and procedures.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all HCCS machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all staff and encouraged for students.

1.3.6 Key responsibilities of students and young people are:

- Contributing to the development of e-safety policies.
- Reading the school/setting Acceptable Use Policy (AUP) and adhering to it.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing e-safety issues.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.3.7 Key responsibilities of parents and carers are:

- Reading the school/setting Acceptable Use Policy, encouraging their students to adhere to it, and adhering to it themselves where appropriate.
- Discussing e-safety issues with their students, supporting the school in their e-safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Using school systems, such as the website, My Child At School, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – [UK Safer Internet Centre](#)

Hot topics – [Childnet International](#)

Parent resource sheet – [Childnet International](#)

2. Online Communication and Safer Use of Technology

2.1 Managing the HCCS website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
- 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 head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including e-safety on the school website.

2.2 Publishing images and videos online

- The school will ensure that all images are used in accordance with the school's image use policy.
- In line with the school's image policy, permission from parents or carers will always be obtained before images/videos of students are electronically published.

2.3 Managing email

- Students may only use HCCS provided email accounts for educational purposes.
- All members of staff are provided with a specific HCCS email address to use for any official communication.
- The use of personal email addresses by staff for any official HCCS 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 must only be sent using secure and encrypted methods.
- Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school e-safety incident log.
- Sensitive or personal information will only be shared via email in accordance with GDPR and data protection legislation.
- Personal email accounts should not be accessed in school and may be blocked.
- School email addresses and other official contact details will not be used for setting up personal social media accounts or signing up to websites/ mailing lists for personal use.

2.4 Appropriate and safe classroom use of the internet and associated devices

- 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.
- Internet use is a key feature of educational access and all students 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.

- The school will instruct staff and students that the use of Internet-derived materials must comply with copyright law and that they must acknowledge the source of information.
- All members of staff are aware that they cannot rely on filtering alone to safeguard students and supervision, classroom management and education about safe and responsible use is essential.
- Students will be appropriately supervised when using technology, according to their ability and understanding.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measures in place.
- 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 the internet to enable students and staff to communicate and collaborate in a safe and secure environment.
- 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.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

3. Social Media Policy

3.1 General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of the HCCS community 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, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the HCCS community 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 HCCS community.
- All members of the HCCS community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control students' access to social media and social networking sites whilst on site and using school provided devices and systems.

- The use of social networking applications during school hours for personal use is not permitted.
- Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the HCCS community on social media sites should be reported to the school leadership team and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of 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 in accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2 Official use of social media

- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.
- Staff will use school provided email addresses to register for and manage official school approved social media channels.
- Members of staff running official school social media channels must ensure they are aware of the required behaviours and expectations of use and that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official school social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official school social media sites will comply with legal requirements including the GDPR, Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use by the school will be in line with existing policies including anti-bullying and child protection.
- Images or videos of students will only be shared on official school social media sites/channels in accordance with the school image use policy.
- Information about safe and responsible use of school social media channels will be communicated clearly and regularly to all members of the school community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website and take place with approval from the Leadership Team.

- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Parents/Carers and students will be informed of any official school social media use, along with expectations for safe use and school action taken to safeguard the community.
- HCCS official social media channels are:
 - **Twitter**
@hccs1978, @HC6F_College, @HccsDofE
 - **Facebook** - <https://www.facebook.com/Holmes-Chapel-Comprehensive-School-Sixth-Form-College-340751732611578/>
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.3 Staff official use of social media

- 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 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 school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any images posted on the school social media channel have appropriate 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 unless they are authorised to do so.
- Staff using social media officially will inform their line manager, the school e-safety (e-Safety) lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.
- Staff using social media officially will read the school Acceptable Use Policy before official social media use will take place.

3.4 Staff personal use of social media

- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with their line manager/ member of the Leadership Team/headteacher.
- If ongoing contact with students is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- All communication between staff and members of the school community on school business will take place via official approved communication channels (such as school email address or phone numbers). Staff must not use personal accounts or information to make contact with students or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Headteacher.
- Any communication from students/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.
- Information staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with school's policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.
- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.
- Members of staff are encouraged not to identify themselves as employees of HCCS on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider school community.
- Members of staff will ensure that they do not represent their personal views as that of the school on social media.
- School email addresses will not be used for setting up personal social media accounts.

3.5 Students use of social media

- Safe and responsible use of social media sites will be outlined for students and their parents as part of the school 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 safe and secure 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 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 students under the age of 13, therefore the School will not create accounts within school specifically for students 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. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

- Please refer to the schools Mobile Phone Policy

5. Use of Generative Artificial Intelligence (AI)

- Please refer to the school's AI policy.

6. Policy Decisions

6.1. Reducing online risks

- HCCS 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 systems are in place to prevent staff and students from accessing unsuitable or illegal content. The school currently uses Smoothwall for this purpose.
- The school also uses Smoothwall Monitor to proactively monitor and alert when users type certain keywords into any school owned device (or personal Chromebook logged into a school account). The alerts are monitored 24/7 by real humans allowing a fast response to any critical safeguarding event.
- 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 or device.
- The school will audit technology use to establish if the e-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 school's leadership team.
- Filtering decisions, internet access and device use by students and staff will be reviewed regularly by the school's leadership team.

6.2. Internet use throughout the wider HCCS community

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site.
- All users of the school systems should expect that their internet use will be monitored and filtered at all times.

6.3 Authorising internet access

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.
- All staff, students and visitors will read and accept the School Acceptable Use Policy before using any school ICT resources.

- Parents will be informed that students will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the School Acceptable Use Policy and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the school community (such as with students with special education needs) the school will make decisions based on the specific needs and understanding of the student(s).

7. Engagement Approaches

7.1 Engagement and education of students and young people

- An e-safety curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst students.
- Education about safe and responsible use will precede internet access.
- Students will be supported in reading and understanding the school Acceptable Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- E-safety will be included in the MyCurriculum and Computing programmes of study covering both safe school and home use.
- The student Acceptable Use expectations and Posters will be posted in all computer rooms.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.

7.2 Engagement and education of students and young people who are considered to be vulnerable

- HCCS is aware that some students may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate e-safety education is given, with input from specialist staff as appropriate (e.g. SENCO).

7.3 Engagement and education of staff

- The e-safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.
- To protect all staff and students, the school will implement an Acceptable Use Policy which highlights appropriate online conduct and communication.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.
- Members of staff with a responsibility for managing filtering systems or monitoring ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.
- The school will highlight useful online tools which staff should use with students in the classroom. These tools will vary according to the age and ability of the students.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

7.4 Engagement and education of parents and carers

- HCCS recognises that parents/carers have an essential role to play in enabling students to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school e-safety policy and expectations in newsletters, letters, the school prospectus and on the school website.
- A partnership approach to e-safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e-safety at other well attended events e.g. parent evenings
- Parents will be requested to read e-safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy and discuss its implications with their students.
- Information and guidance for parents on e-safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their students online.

8. Managing Information Systems

8.1 Managing personal data online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act and GDPR.
- Full information regarding the schools approach to data protection and information governance can be found in the school's data protection policy.

8.2 Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus and malware protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The Strategic ICT Manager will review system capacity regularly.
- The appropriate use of user logins and passwords to access the school network will be enforced.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record internet use on all school owned devices the logs are created and held by our onsite Smoothwall.

8.3 Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and students must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff and students will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- We require staff to use strong passwords and, where available, 2 factor authentication for access into our system.
- We advise students to use strong passwords for access into our system.
- We advise staff and students that passwords should be unique for each different system they use. Use of a password manager is encouraged to help with this.
- Staff and students must never write passwords down.

8.4 Filtering Decisions

- The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our students, with advice from technical, educational and safeguarding staff.
- The school uses secure broadband connectivity which is filtered by the school and appropriate to the age and requirement of our students.

- The school uses a Smoothwall filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
- The school will ensure that age and ability appropriate filtering is in place whilst using school devices and systems to try and prevent staff and students from being accidentally or deliberately exposed to unsuitable content.
- The school will work to ensure that the filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all students) will be made aware of.
- If staff or students discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Cheshire Police or CEOP immediately.

8.5 Management of applications (apps) used to record students's progress

- The headteacher is ultimately responsible for the security of any data or images held of students.
- Apps/systems which store personal data will be risk assessed prior to use.
- Personal staff mobile phones or devices will not be used for any apps which record and store students' personal details, attainment or photographs on the device.
- Only school issued devices will be used for apps that record and store student's personal details, attainment or photographs on the device.
- Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

9. Responding to Online Incidents and Concerns

- All members of the school/setting community will be informed about the procedure for reporting e-safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The Designated Safeguarding Lead (DSL) will be informed of any e-safety incidents involving child protection concerns, which will then be recorded.
- The Designated Safeguarding Lead (DSL) will ensure that e-safety concerns are escalated and reported to relevant agencies.

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online bullying will be dealt with under the School's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the head teacher
- Students, parents and staff will be informed of the school's complaints procedure.
- Staff will be informed of the complaints and whistleblowing 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 e-safety incidents in accordance with the school 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 Cheshire Police (via 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 Cheshire Police.
- If the school is unsure how to proceed with any incidents of concern, then advice will be sought from Cheshire East.
- Parents and students will need to work in partnership with the school to resolve issues.

9.1 Procedures for Responding to Specific Online Incidents or Concerns

The following content is provided to enable schools and education settings to make appropriate safeguarding decisions regarding e-safety concerns and has been adapted from the document written by the Kent e-Safety Strategy Group with input from specialist services and teams. This content is not exhaustive and cannot cover every eventuality so professional judgement and support from appropriate agencies is encouraged.

9.1.1 Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

- HCCS ensures that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating incident images of students (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.
- HCCS views “sexting” as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If the school are made aware of an incident involving indecent images of a child the school will:
 - Act in accordance with the school’s child protection and safeguarding policy.
 - Immediately notify the designated safeguarding lead.
 - Store the device securely.
 - Carry out a risk assessment in relation to the students(s) involved.
 - Consider the vulnerabilities of students(s) involved (including carrying out relevant checks with other agencies)
 - Make a referral to student's social care and/or the police (as needed/appropriate).
 - Put the necessary safeguards in place for students 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.
 - Implement appropriate sanctions in accordance with the school's 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.
- The school will not view the image unless there is a clear need or reason to do so.
- The school will not send, share or save indecent images of students and will not allow or request students to do so.
- If an indecent image has been taken or shared on the HCCS network or devices, then the school will take action to block access to all users and isolate the image.
- The school will need to involve or consult the police if images are considered to be illegal.
- The school will take action regarding indecent images, regardless of the use of HCCS equipment or personal equipment, both on and off the premises.
- The school will follow the guidance (including the decision making flow chart and risk assessment template) as set out in “‘Sexting’ in schools: advice and support around self-generated images. What to do and how to handle it”.

- The school will ensure that all members of the community are aware of sources of support.
- If students at other schools are believed to have been targeted, then the school will seek support from Cheshire East to enable other schools to take appropriate action to safeguard their community.

9.1.2 Responding to concerns regarding Online Child Sexual Abuse

- HCCS 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 students 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 students, staff and parents/carers.
- HCCS views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately from Cheshire Police.
- 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 school's child protection and safeguarding policy.
 - Immediately notify the designated safeguarding lead.
 - Store any devices involved securely.
 - Immediately inform Cheshire police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: <http://www.ceop.police.uk/safety-centre/>
 - Where appropriate the school will involve and empower students to report concerns regarding online child sexual abuse
 - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
 - Make a referral to student'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 Cheshire East 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 students and other members of the school community, for example including the CEOP report button on the school website homepage.

9.1.3 Responding to concerns regarding Indecent Images of Students

- HCCS will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Students including the possible consequences.
- The school will take action regarding Indecent Images of Students regardless of the use of HCCS equipment or personal equipment, both on and off the premises.
- The school will take action to prevent access to Indecent Images of Students for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering and firewalls.
- If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately from Cheshire Police.
- If HCCS is made aware of Indecent Images of Students then the school will:
 - Act in accordance with the school's child protection and safeguarding policy.
 - Immediately notify the school Designated Safeguard Lead.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF) and Cheshire police via 101 (using 999 if a child is at immediate risk).
- If the school are made aware that a member of staff or a student has been inadvertently exposed to indecent images of students whilst using the internet then the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
- If the school are made aware that indecent images of students have been found on the school's electronic devices then the school will:
 - Ensure that the Designated Safeguard Lead is informed.

- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and students'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.
- If the school are made aware that a member of staff is found in possession of indecent images of students on their electronic device provided by the school, then the school will:
 - Ensure that the Designated Safeguard Lead 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.
 - Follow the appropriate school policies regarding conduct.

9.1.4 Responding to concerns regarding radicalisation or extremism online

- The school will take all reasonable precautions to ensure that students 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 Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.

9.1.5 Responding to concerns regarding cyberbullying

- Cyberbullying, along with all other forms of bullying, of any member of the HCCS 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 Designated Safeguarding Lead will obtain advice immediately from Cheshire Police.
- Students, staff and parents/carers will be advised to keep a record of the bullying 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.
 - Parents/carers of students involved in online bullying will be informed.
 - The Police will be contacted if a criminal offence is suspected.