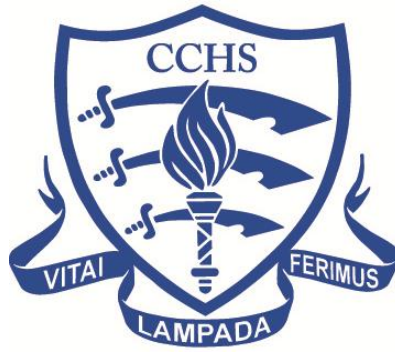


Chelmsford County High School for Girls



Online Safety and Data Security Policy

Guidance for ICT Acceptable Use

Approved by the Trustee Body: July 2026

CONTENTS

SCOPE	- 3 -
PROCESS FOR MONITORING THE IMPACT OF THE ONLINE SAFETY POLICY	- 3 -
MONITORING	- 4 -
ACCEPTABLE USE AGREEMENT: CHELMSFORD COUNTY HIGH SCHOOL FOR GIRLS	- 5 -
ACCEPTABLE USE AGREEMENT: STAFF, TRUSTEES AND VISITORS	- 7 -
COMPUTER VIRUSES.....	- 8 -
SECURITY.....	- 8 -
IMPACT LEVELS AND PROTECTIVE MARKING	- 9 -
SENIOR INFORMATION RISK OWNER (SIRO)	- 9 -
INFORMATION ASSET OWNER (IAO)	- 9 -
THE USE OF ARTIFICIAL INTELLIGENCE (AI) SYSTEMS IN SCHOOL	- 11 -
E-MAIL.....	- 13 -
MANAGING EMAIL.....	- 13 -
SENDING EMAILS	- 14 -
RECEIVING EMAILS	- 14 -
EMAILING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION	- 14 -
EQUAL OPPORTUNITIES.....	- 15 -
STUDENTS WITH ADDITIONAL NEEDS	- 15 -
ESAFETY.....	- 16 -
ESAFETY - ROLES AND RESPONSIBILITIES	- 16 -
ESAFETY IN THE CURRICULUM.....	- 16 -
ESAFETY SKILLS DEVELOPMENT FOR STAFF	- 17 -
MANAGING THE SCHOOL ESAFETY MESSAGES	- 17 -
INCIDENT REPORTING, ESAFETY INCIDENT LOG & INFRINGEMENTS	- 18 -
INCIDENT REPORTING	- 18 -
CYBER SECURITY	- 18 -
BREACHES.....	- 20 -
ESAFETY INCIDENT LOG	- 20 -
INTERNET ACCESS	- 22 -
MANAGING THE INTERNET	- 22 -
INTERNET USE	- 22 -
INFRASTRUCTURE.....	- 23 -
MANAGING OTHER WEB 2 TECHNOLOGIES	- 24 -
PARENTAL INVOLVEMENT	- 25 -
PASSWORDS AND PASSWORD SECURITY.....	- 26 -
PASSWORD POLICY.....	- 26 -
ZOMBIE ACCOUNTS	- 27 -
PERSONAL OR SENSITIVE INFORMATION.....	- 28 -
PROTECTING PERSONAL, SENSITIVE, CONFIDENTIAL AND CLASSIFIED INFORMATION	- 28 -
STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE MEDIA.....	- 28 -
REMOTE ACCESS	- 29 -
REMOTE LEARNING	- 30 -
SAFE USE OF IMAGES.....	- 31 -
TAKING OF IMAGES AND FILM.....	- 31 -

PUBLISHING STUDENT'S IMAGES AND WORK	- 31 -
STORAGE OF IMAGES	- 31 -
WEBCAMS AND CCTV	- 31 -
SCHOOL ICT EQUIPMENT INCLUDING PORTABLE & MOBILE ICT EQUIPMENT & REMOVABLE MEDIA	- 32 -
SCHOOL ICT EQUIPMENT	- 32 -
PORTABLE & MOBILE ICT EQUIPMENT	- 32 -
MOBILE TECHNOLOGIES	- 33 -
<i>Personal Mobile Devices (including phones)</i>	- 33 -
<i>School Provided Mobile Devices (including phones)</i>	- 34 -
REMOVABLE MEDIA	- 34 -
SCHOOL IT DEVICE LOAN AGREEMENT	- 35 -
SERVERS	- 36 -
DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY	- 37 -
1.PURPOSE	- 37 -
2. RESPONSIBILITIES	- 37 -
3. ASSET IDENTIFICATION	- 37 -
4. DATA BACKUP AND MEDIA SANITISATION	- 38 -
5. DISPOSAL CRITERIA	- 38 -
6. THIRD PARTY SERVICE PROVIDERS	- 38 -
7. ENVIRONMENTAL RESPONSIBILITY.....	- 38 -
SYSTEMS AND ACCESS	- 39 -
TELEPHONE SERVICES	- 40 -
MOBILE PHONES	- 40 -
CURRENT LEGISLATION.....	- 41 -
ACTS RELATING TO MONITORING OF STAFF EMAIL	- 41 -
OTHER ACTS RELATING TO ESafety.....	- 41 -
ACTS RELATING TO THE PROTECTION OF PERSONAL DATA.....	- 44 -

Scope

This Online Safety Policy outlines the commitment of Chelmsford County High School [The School] to safeguard members of our school community online in accordance with statutory guidance and best practice. This Online Safety Policy applies to all members of the school community (including staff, learners, trustees, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Trustee

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, Emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the Email or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA), the Lawful Business Practice Regulations 2000, the Freedom of Information Act 2000, The Communications Act 2003, The Education and Inspections Act 2011, The Serious Crime Act 2015, The Criminal Justice and Courts Act 2015 and the Online Safety Act 2025

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Acceptable Use - Agreement / eSafety Rules

- I will only use ICT systems in school, including the internet, Email, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the School network/ Learning Platform with my own user name and password.
- I will follow the School's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my School Email address for school-related matters.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher or other responsible adult.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

On CCHS headed paper

Dear Parent/ Carer

ICT including the internet, VLE, Email and mobile technologies have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of eSafety and know how to stay safe when using any ICT.

Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their Tutor, Year Leader or the Deputy Headteacher – Pastoral.

Please return the bottom section of this form to school for filing.

This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full on our website.

✂

Student and Parent/ Carer Agreement

We have discussed this document and(student name) agrees to follow the eSafety rules and to support the safe and responsible use of ICT at Chelmsford County High School. My daughter understands that these rules are designed to keep her safe and that if they are not followed, School sanctions will be applied and that I may be contacted.

Parent/ Carer Signature

Student Signature.....

Form Date

Acceptable Use Agreement: Staff, Trustees and Visitors

Staff, Trustee and Visitor

Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as Email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Deputy Headteacher - Pastoral or the Business Manager (acting on behalf of the Headteacher who is the Senior Information Risk Owner.)

- I will only use the school's email / internet / Intranet / VLE and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Trustee Body.
 - I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
 - I will ensure that all electronic communications with students and staff are compatible with my professional role.
 - I will not give out my own personal details, such as mobile phone number, personal Email address and social networking identities to students.
 - I will only use the approved, secure Email system(s) for any school business.
 - Trustees may, on exception, use personal emails where matters are of a time sensitive nature and they cannot access their School accounts. In all instances, school accounts should be copied into the communications and only retained on those accounts. Communications may not include any information that is deemed as sensitive personal data.
 - I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Trustee Body. I will not install any hardware or software without the permission of the Network manager
 - I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
 - Images of students and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the School network without the permission of the parent/ carer, member of staff or Headteacher.
 - I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request at the Headteacher's instigation to my Line Manager or Headteacher.
 - I will respect copyright and intellectual property rights.
 - I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
 - I will support and promote the school's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
 - I understand this forms part of the terms and conditions set out in my contract of employment
- This Acceptable Use Agreement is a summary of our eSafety Policy which is available in full on the School website.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature Date

Full Name (Printed)

Job Title

Computer Viruses

- All files downloaded from the internet, received via Email or on removable media must be checked for any viruses using school provided anti-virus software before using them.
 - Never interfere with any anti-virus software installed on school ICT equipment that you use.
 - If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team,
 - If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know,
-

Security

- The School gives relevant staff access to its Management Information System, with a unique ID and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the Policy for ICT Acceptable Use.
- The Senior Information Risk Owner (SIRO) is the Headteacher, however day to day responsibility for the SIRO actions and Asset Information Owner(s) (AIO) is delegated to the Business Manager and the Network Manager respectively.
- Use of removable media is only possible with exceptional approval that can be requested via the Network Manager.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents, copied, scanned or printed.
- Communication by fax is not deemed secure and should not be used.

Impact Levels and Protective Marking

- Appropriate labelling of data should help schools secure data and so reduce the risk of security incidents.
- Apply labelling in accordance with guidance from your Senior Information Risk Owner (SIRO) or their delegate.
- Most learner or staff personal data will be classed as Protect, although some data e.g. Child Protection data, should be classed as Restricted.
- Protect/Restrict and caveat classifications that schools may use are;
 - PROTECT – PERSONAL e.g. personal information about an individual
 - PROTECT – APPOINTMENTS e.g. to be used for information about visits from the Queen or government ministers
 - PROTECT – LOCSEN e.g. for local sensitive information
 - PROTECT – STAFF e.g. Organisational staff only
 - RESTRICTED e.g. sensitive personal information about an individual
- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business.
- The protective mark should be in bold capital letters within the header and footer of each page of a document.
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset.
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents.

Reviews are continuing to look at the practical issues involved in applying protective markings to electronic and paper records and government representatives are working with suppliers to find ways of automatically marking reports and printouts.

Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who is familiar with information risks and the school's response. Typically, the SIRO should be a member of the senior leadership team and have the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

The SIRO at CCHS is the Headteacher, however day to day management of these responsibilities is delegated to the Business Manager

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of

learners and staff; such as assessment records, medical information and special educational needs data. Schools should identify an Information Asset Owner. For example, the school's Management Information System (MIS) should be identified as an asset and should have an Information Asset Owner. In this example the MIS Administrator or Manager could be the IAO.

The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, student or staff etc. including unique identifiers)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several IAOs, whose roles may currently be those of e-safety coordinator, ICT manager or Management Information Systems administrator or manager.

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action. The IAO is the Network Manager.

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Policy Statements

- The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.

- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

E-mail

The use of Email within most schools is an essential means of communication for both staff and students. In the context of school, Email should not be considered private. Educationally, Email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an Email in relation to their age and good network etiquette; 'netiquette'.

Managing Email

- The school gives all staff and students their own Email account to use for all school business as a work-based tool This is to minimise the risk of receiving unsolicited or malicious Emails and avoids the risk of personal profile information being revealed.
- For the safety and security of users and recipients, all mail is filtered and logged; if necessary Email histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact students, parents or conduct any school business using personal Email addresses.
- All Emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Emails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000, a Subject Access Request (SAR) or Environmental Information Request (EIR) under the Data Protection Act 2018. You must therefore actively manage your Email account as follows:
 - Delete all Emails of short-term value
 - Organise Email into folders and carry out frequent house-keeping on all folders and archives
- All student Email users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in Email communication, or arrange to meet anyone without specific permission and should virus checking attachments.
- Students must immediately tell a teacher/ trusted adult if they receive an offensive Email.
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive Email.
- Students are introduced to Email as part of the ICT Scheme of Work.
- However you access your school Email (whether directly, through webmail when away from the office or on non-school hardware) all the school Email policies apply,

Sending Emails

- Use your own school Email account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of Email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- An outgoing Email greater than twenty megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming Email.
- School Email is not to be used for personal advertising.

Receiving Emails

- Check your Email regularly.
- Never open attachments from an untrusted source; Consult your network manager first.
- Do not use the Email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding or deletion of Emails is not allowed.

Emailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using Email. Emailing confidential data is not recommended and should be avoided wherever possible.
- Where your conclusion is that Email must be used to transmit such data:
 - Obtain express consent from your manager to provide the information by Email
 - Exercise caution when sending the Email and always follow these checks before releasing the Email:
 - Verify the details, including accurate Email address, of any intended recipient of the information
 - Verify (by phoning) the details of a requestor before responding to Email requests for information
 - Do not copy or forward the Email to any more recipients than is absolutely necessary
 - Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
 - Request confirmation of safe receipt.

Students with Additional Needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. internet activities are planned and well managed for these children and young people.

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and Trustees have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is the Deputy Headteacher- Pastoral who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as ECC, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Trustees are updated by the Head/ eSafety co-ordinator and all Trustees have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, Trustees, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHE

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the students on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in ICT and PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities.
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button. All students are aware of their digital footprint and parents are reminded during Meet the Tutor Evening presentations.
- Students are taught to critically evaluate materials and learn good searching skills through

cross curricular teacher models, discussions and via the ICT curriculum.

eSafety Skills Development for Staff

- New staff receive information on the School's Acceptable Use Policy as part of their induction.
 - All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart).
 - All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.
-

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used.

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's SIRO or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner.

Incidents relating to data security should be reported through the GDPR toolkit available on the staff intranet, or through notification to the Business Manager

All suspicious activity that could be an indication of a Cyber-attack should be escalated as a matter of priority to the IT Team and Business Manager who will then follow the Cyber Security Incident Response Plan. Examples of suspicious activity includes, but is not limited to:

- A. Email or phone notification from an intrusion detection tool.
- B. Suspicious entries in system or network accounting, or logs.
- C. Discrepancies between logs.
- D. Repetitive unsuccessful logon attempts within a short time interval.
- E. Unexplained new user accounts.
- F. Unexplained new files or unfamiliar file names.
- G. Unexplained modifications to file lengths and/or dates, especially in system files.
- H. Unexplained attempts to write to system files or changes in system files.
- I. Unexplained modification or deletion of data.
- J. Denial/disruption of service or inability of one or more users to login to an account.
- K. System crashes.
- L. Poor system performance of dedicated servers.
- M. Operation of a program or sniffer device used to capture network traffic.
- N. Unusual time of usage (e.g. users login during unusual times)
- O. Unusual system resource consumption. (High CPU usage)
- P. Last logon (or usage) for a user account does not correspond to the actual last time the user used the account.
- Q. Unusual usage patterns (e.g. a user account associated with a user in Finance is being used to login to an HR database).
- R. Unauthorized changes to user permission or access.

Cyber Security

[The DfE Cyber security standards for schools and colleges explains:](#)

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes

- a significant data breach
 - significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
 - financial loss
 - reputational damage”
- the school has reviewed the DfE Cyber security standards for schools and colleges and meets these standards
 - the school will conduct a cyber risk assessment annually and review each term
 - the school, has identified the most critical parts of the school’s digital and technology services and sought assurance about their cyber security
 - the school has an effective backup and restoration plan in place in the event of cyber attacks
 - the school’s governance and IT policies reflect the importance of good cyber security
 - staff and Governors receive training on the common cyber security threats and incidents that schools experience
 - the school’s education programmes include cyber awareness for learners
 - the school has a business continuity and incident management plan in place
 - there are processes in place for the reporting of cyber incidents.
 - All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

Breaches

A breach or suspected breach of policy by a School employee, contractor, volunteer, trustee or student may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

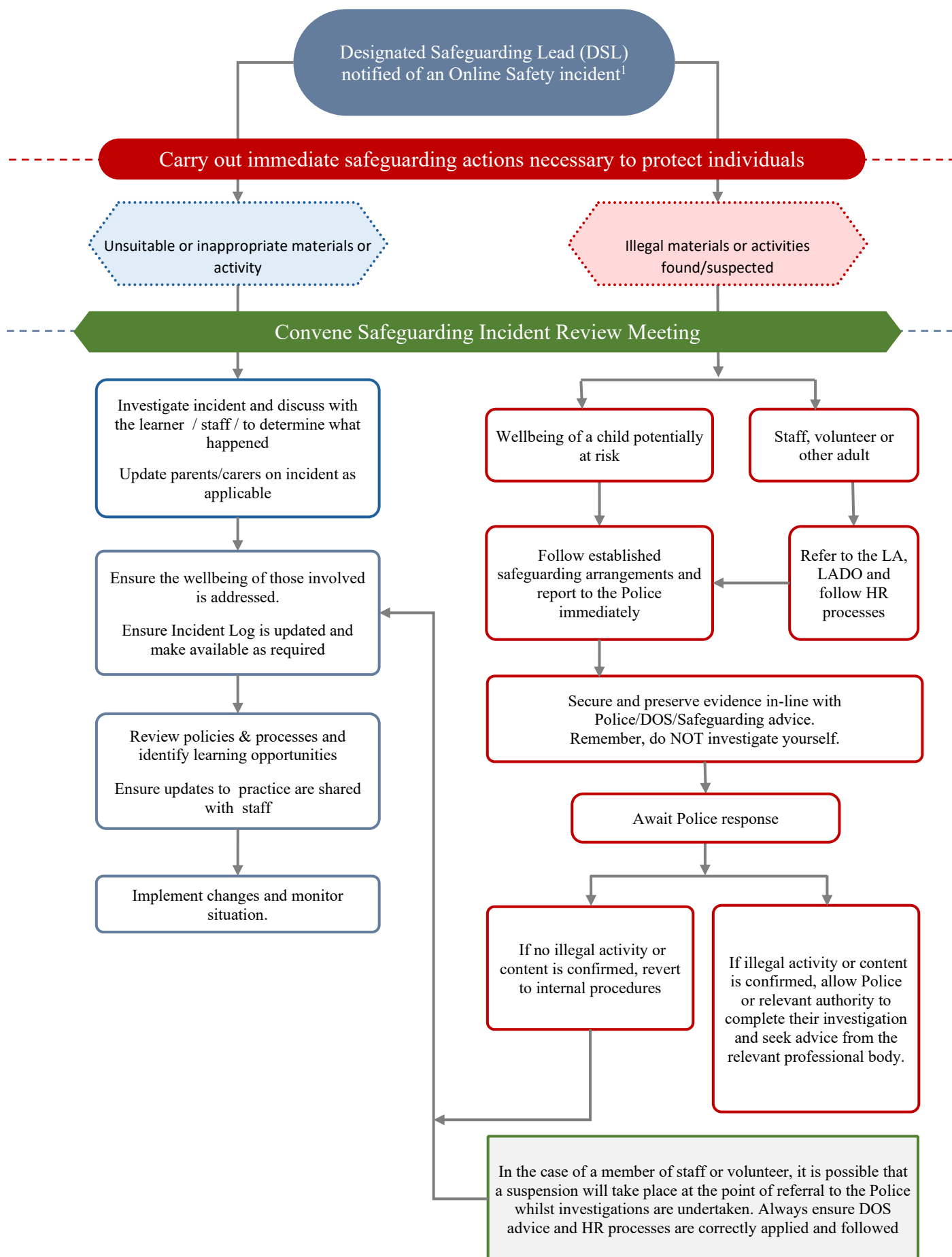
eSafety Incident Log

Some incidents may need to be recorded in other places, such as MyConcern, if they relate to a bullying, racist or other serious incident that relates to safeguarding concerns

Misuse and Infringements

Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. All incidents should be logged.



Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **Internet** is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

The DfE guidance (for England) on filtering and monitoring in “[Keeping Children Safe in Education](#)” states:

“It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children’s exposure to the ... risks from the school’s or college’s IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified...”

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published [filtering and monitoring standards...](#)”

Managing the internet

- The school maintains students who will have supervised access to internet resources (where reasonable) through the school’s fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with students.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Don’t reveal names of colleagues, students, contractors, trustees or clients or any other confidential information acquired through your job on any social networking site or blog.

- On-line gambling or gaming is not allowed.

It is at the Headteacher's discretion what internet activities are permissible for staff and students and how this is disseminated.

Infrastructure

- Our school also employs some additional web filtering which is the responsibility of the Network Manager.
- Blocked sites can be unblocked providing the request comes from a teacher with a business case for the site to be unblocked, and the IT department agree that the website is appropriate for a school environment. Where the IT department are unable to make a decision, this will be escalated to a member of SLT for a final decision.
- CCHS is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and students are aware that school-based email and internet activity can be monitored and explored further if required.
- The school uses management control tools for controlling and monitoring workstations.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.
- Removable media is not permitted for use, except by exceptional approval. Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the School's responsibility nor the network manager's to install or maintain virus protection on personal systems. If students or staff wish to bring in work on removable media it must be given to the IT Department for a safety check first and exceptional access given by the IT Department where there is a valid need to remove the block on usage.
- Students and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the IT Department.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed using the IT helpdesk.

Managing Other Web 2 Technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online. Students are taught about the importance of their digital footprint.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our students are asked to report any incidents of bullying to the School.
- Staff may only create blogs, twitter accounts or other social media or communication methods in order to communicate with students in accordance with School protocol as approved by the Headteacher.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and students are actively encouraged to contribute to adjustments or reviews of the school eSafety policy through Student Voice, Sixth Form Council and feedback at the Meet the Tutor Evenings.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website).
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
 - Information and celebration evenings
 - Posters
 - Website/ Learning Platform postings
 - Newsletter items

Passwords and Password Security

Password Policy

All users, inclusive of employees, subcontractors and suppliers with direct access to CCHS's information technology systems are expected to conform to this policy.

CCHS's IT Team are responsible for providing support to users in complying with this policy.

The IT Manager is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated.

Default Credentials

CCHS always changes default credentials. Default credentials are changed as a matter of priority upon receiving a new device, factory resetting a device, or commissioning a new service. Accounts and devices are never exposed to the internet before first having their default credentials changed.

Strong Passwords

CCHS follows the following principles when creating a new password.

- Are never obvious (easy for an attacker to guess)
- Are never commonly used passwords
- Have never been disclosed in a breach (validated using the HaveIBeenPwned service (haveibeenpwned.com))
- Are never re-used when a password expires
- Are never re-used across different accounts
- Meets the complexity requirements:
 - Minimum of 8 characters in length
 - Contains a minimum of one lowercase character, one uppercase character and one number.
 - does not contain any part of the user's name

Password Disclosure

CCHS staff and students will never:

- Write down their passwords or encryption keys
- Disclose their password to others

CCHS's IT Team will never ask staff and students for their password.

Multi-Factor Authentication

All staff and Students at CCHS will ensure that multi-factor authentication (MFA) is enabled for all devices and services that support this technology. CCHS's preferred method of MFA is via a notification on the Microsoft authenticator app.

Training

All staff and students at CCHS are encouraged to remain conversant with password and other cybersecurity advice from the UK's National Cyber Security Centre.

Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left. This should be within one month of a staff member leaving and six months of normal student transfer phases, or immediate if intra-year. Some special exceptions can be granted if agreed with SLT.
- Prompt action on disabling accounts will prevent unauthorized access.
- Regularly change generic passwords to avoid unauthorized access (Microsoft® advise every 42 days).

Further advice available <http://www.itgovernance.co.uk/>

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared devices (e.g. multi-function print, scan and copiers) are used and when access is from a non-school environment.
- Only download personal data from systems if expressly authorised to do so by your manager.
- You must not post personal, sensitive, confidential, or classified information on the internet, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Store all removable media securely.
- Securely dispose of removable media that may hold personal data.
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

Remote Access

- You are responsible for all activity via your remote access facility.
- Only use equipment with an appropriate level of security for remote access.
- Multi Factor Authentication (MFA) is required to log onto remote access. This is done via the authenticator app, in the same way MFA works for Office 365 services.
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- Protect School information and data at all times, ensuring that any sensitive data is protected from view of any persons who may be able to view your screen. Take particular care when access is from a non-School environment. Printing is only available from remote access to the school's printers, and printing to personal devices is disabled.
- Copying files to and from remote access is disabled. It is not possible to copy any files to or from your personal machine into the remote access system.

Remote Learning

- Where teaching or learning is required to take part remotely, staff and students must conduct themselves in the same way as if they were on site in a classroom.
- Where possible, users should blur their background in order to maintain privacy.
- Where lessons are required to be recorded, permission should be sought of all users to ensure that they consent to being recorded.
- Where recordings are saved, it must be ensured that the recordings are saved in a secure area, and only seen by relevant staff/students. It must be ensured that their recordings are not shared outside the school network.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

Staff should be aware of the privacy notices that relate to usage of images and film, available on our website <http://www.cchs.co.uk/about-us/privacy-notices/>

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.
- Staff are permitted in some circumstances as agreed by the Headteacher, to use personal digital equipment, such as mobile phones and cameras, to record images of students, this is particularly when accompanying students on trips and visits. When back in school they will be transferred onto the school system and deleted off the personal phone/camera. Students are permitted, under the guidance of their teacher, to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips.

Publishing Student's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's photos for CCHS publications, publicity and possible local and national media/ press releases. Usage of these photos must be in accordance with the parental permission / denial and with our privacy notices.

Storage of Images

- Images/ films of children are stored on the school's network.
- Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network/ Learning Platform.
- **The IT Manager** has the responsibility of deleting the images when they are no longer required, or the student has left the school.

Webcams and CCTV

- The school uses CCTV for security and safety. Access to this is permitted only in accordance with our CCTV privacy notice <http://www.cchs.co.uk/about-us/privacy-notices/>
- We do not use publicly accessible webcams in school.

Webcams in school are only ever used for specific learning purposes.

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory.
- Ensure that all ICT equipment that you use is kept physically secure.
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.
- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive.
- Personal or sensitive data should not be stored on the local drives of desktop PCs.
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles.
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager or the IT Department. You must also provide details of all your system logons so that they can be disabled.
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
 - maintaining control of the allocation and transfer within their Unit
 - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all school data is stored on school's network, and not kept solely on

the laptop. Any equipment where personal data is likely to be stored must be encrypted.

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device except in the case of an emergency where there is no other alternative.
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes whilst on school grounds. At all times the device must be turned off unless permission has been granted for medical purposes. This technology may be used, however for educational purposes, as mutually agreed with the class teacher for those in the sixth form. All students, without medical exemption, must otherwise keep phones securely locked during the school day in pouches purchased. Students with medical, or other, exemptions may only use their devices for the agreed purpose. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

Removable Media

Removable Media is not permitted without exceptional approval for a valid purpose. Access to use removable media can only be granted by the ICT support team with SIRO approval. If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media' – Pages- 28 - 37

- Only use recommended removable media.
- Store all removable media securely.
- Removable media must be disposed of securely by your ICT support team.



Chelmsford County High School *for* Girls
SCHOOL IT DEVICE LOAN AGREEMENT

We are loaning you this device for the benefit of your child in supporting and developing their education whilst they are unable to attend school or for use to support their normal way of working, as agreed with the SENDCO.. Other individuals, including children, are not permitted to use the device.

- The device is the property of Chelmsford County High School
- Parents / guardians are responsible for monitoring use of the device and any ensure that the student does not access inappropriate sites, including gaming, at any time.
- You must not decorate or change the external face of the equipment provided in any way, including affixing stickers.
- The school is not responsible for any costs resulting from the use of the computer and the connectivity equipment, including electricity, printer cartridges, paper or any cost occurring from an internet service not provided by the school.
- You must monitor the use of the device and ensure that access is only to educational platforms. Inappropriate use may result in the device loan being withdrawn.
- You must not install any new software, or download any content from the internet, without express permission from the IT team.
- You must not in any way change the settings on firewalls or anti-virus software.
- You must ensure that the Microsoft and antivirus updates are processed.
- Reasonable health and safety precautions should be taken when using a computer. The school is not responsible for any damage to person or property resulting from the device or equipment loaned.
- Keep food and drink away from the device. Do not expose the device to direct sunlight or extreme cold.
- You have a responsibility to take reasonable care to ensure the security of the computer and connectivity equipment. If the device is lost, damaged or stolen, this will not be covered by School's insurance and you will be required to provide a suitable replacement agreed with School.

Device type:	Serial number:
Loan from date:	Return date:
Student name:	Student form:

I have read and understand the above terms and conditions and understand that by breaching the conditions the loan of the device may be withdrawn by the school.

Signed (Parent/Guardian) _____ Date _____

Printed Name _____

Signed (Student) _____ Date _____

Servers

- Newly installed servers holding personal data should be encrypted, therefore password protecting data.
- Always keep servers in a locked and secure environment.
- Limit access rights to ensure the integrity of the standard build.
- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine's specification.
- Back up tapes should be encrypted by appropriate software.
- Data must be backed up regularly.
- Back up tapes/discs must be securely stored in a fireproof container.
- Back up media stored off-site must be secure.
- Remote backups should be automatically securely encrypted.
- Regular updates of anti-virus and anti-spyware should be applied.
- Records should be kept of when and which patches have been applied.
- Ensure that web browsers and other web-based applications are operated at a minimum of 256 BIT cipher strength.

Disposal of Redundant ICT Equipment Policy

1. Purpose

This is an internal policy that defines how Chelmsford County High School for Girls (CCHS) manages the secure and responsible disposal of IT assets. This policy is part of CCHS's aim to ensure an effective IT Asset Management lifecycle.

2. Responsibilities

All users, inclusive of employees, subcontractors and suppliers with direct access to CCHS's information technology systems are expected to conform to this policy.

CCHS's IT service provider is responsible for providing support to users in complying with this policy.

The IT Manager is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated.

Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

<http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx>

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=e

Data Protection Act 2018

<https://ico.org.uk/for-organisations/guide-to-data-protection/>

Electricity at Work Regulations 1989

http://www.opsi.gov.uk/si/si1989/uksi_19890635_en_1.htm

3. Asset Identification

This policy seeks to address the disposal of all of CCHS's information assets that have the capability to record or store data, including:

- PCs
- Laptops
- Servers
- Mobile Phones/Tablets
- Firewalls/Routers/Switches
- Printers/Scanners/Fax Machines
- USB Flash Drives/External Hard Drives

All assets marked for disposal must be identified and agreed for disposal by The IT Manager and Business Manager before any disposal takes place. Where possible, all details such as make, model, serial number and asset number should be recorded in the asset disposal register.

4. Data Backup and Media Sanitisation

CCHS's IT assets should not be disposed of before ensuring that the required data backups and backup tests are done. All media with the capability to record or store data must be properly sanitised according to the sensitivity of the data.

5. Disposal Criteria

CCHS's administration should be notified if any IT equipment needs to be decommissioned. A decision should be made to either reuse/recycle or dispose. Before any equipment is disposed, a risk-based approach should be taken based on the type of asset and the sensitivity of the data potentially stored.

- **Restricted** - Assets used for the processing and storage of restricted and/or personal data should be identified as high risk because data loss could potentially have significantly detrimental effects. Such assets should be properly sanitised using approved technology or physically destroyed.
- **Confidential** - Assets used for the processing and storage of confidential data should be identified as high risk as data loss could also potentially have significantly detrimental effects. Such assets should be properly sanitised using approved technology or physically destroyed.
- **Internal** - Assets used for the processing and storage of internal data should be identified as medium risk. Such assets should be sanitised using approved technology.
- **Public** - Assets used for the processing and storage of public data should be identified as low risk. Such assets should be sanitised and could potentially be reused somewhere else.

6. Third Party Service Providers

Where incapacitated, an approved licensed third-party service provider is contracted to undertake the IT disposal process on behalf of CCHS. This will continue to be monitored to ensure that CCHS's IT disposal standards are met.

Where assets are disposed by a third-party service, certificates of secure destruction will be obtained from the third party service and stored for future reference.

7. Environmental Responsibility

CCHS is fully aware of the hazardous impact of incorrectly discarding electronic equipment. Reasonable care should be taken to thoroughly separate and isolate toxic chemicals and components from all electronic equipment before shipment to a landfill.

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC.
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you.
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time.
- Do not introduce or propagate viruses.
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or ECC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Equality Act, Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act),
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act or Subject Access Requests.

Telephone Services

- You may make or receive personal telephone calls provided:
 1. they are infrequent, kept as brief as possible and do not cause annoyance to others
 2. they are not for profit or to premium rate services
 3. they conform to this and other relevant School policies.
- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

Mobile Phones

- You are responsible for the security of your school mobile phone. Always set the PIN code on your school mobile phone and do not leave it unattended and on display (especially in vehicles).
- Report the loss or theft of any school mobile phone equipment immediately.
- The school remains responsible for all call costs until the phone is reported lost or stolen.
- You must read and understand the user instructions and safety points relating to the use of your school mobile phone prior to using it.
- School SIM cards must only be used in school provided mobile phones.
- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default.
- You must not send text messages to premium rate services.
- In accordance with the Finance Policy on the private use of School provided mobiles, you must reimburse the School for the cost of any personal use of your school mobile phone. This includes call charges incurred for incoming calls whilst abroad. Never use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 emergency calls may be made if it would be unsafe to stop before doing so.

Current Legislation

Acts Relating to Monitoring of Staff Email

Data Protection Act 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

<http://www.hmso.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.legislation.gov.uk/ukpga/2000/23/contents>

Human Rights Act 1998

<http://www.legislation.gov.uk/ukpga/1998/42/contents>

Other Acts Relating to eSafety

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of

causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

The Online Safety Act 2023

The Online Safety Act 2023 (the Act) protects children and adults online. It puts a range of new duties on social media companies and search services, giving them legal duties to protect their users from illegal content and content harmful to children. The Act gives providers new duties to implement systems and processes to reduce risks their services are used for illegal activity, and to take down illegal content when it does appear.

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith; or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

<http://www.legislation.gov.uk/ukpga/2006/1/contents>

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

<http://www.legislation.gov.uk/ukpga/2003/42/contents>

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

<http://www.legislation.gov.uk/ukpga/2003/21/contents>

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)

- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

<http://www.legislation.gov.uk/ukpga/1990/18/contents>

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (Email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

<http://www.legislation.gov.uk/ukpga/1988/27/contents>

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining their author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

<http://www.legislation.gov.uk/ukpga/1988/48/contents>

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

<http://www.legislation.gov.uk/ukpga/1986/64/contents>

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

<http://www.legislation.gov.uk/ukpga/1978/37/contents>

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

1964 - <http://www.legislation.gov.uk/ukpga/1964/74/contents>

1959 - <http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents>

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

<http://www.legislation.gov.uk/ukpga/1997/40/contents>

Acts Relating to the Protection of Personal Data

Data Protection Act 2018

<https://www.gov.uk/data-protection>

The Freedom of Information Act 2000

<https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/>