COLCHESTER COUNTY HIGH SCHOOL FOR GIRLS

Policy No. 44. e-SAFETY POLICY

COMMITTEE	Curriculum & Student Matters
LINK GOVERNOR	Mr Paul Archer
SLT RESPONSIBLE	Mrs Dawn Frost Associate Principal
REVIEW	Every 2 Years or following changes to Statutory Guidance
POLICY REVIEWED	May 2025
REVIEW DUE	May 2027
APPROVED BY THE GOVERNING BODY	June 2025

Key Personnel

e-Safety Coordinator	Mr Casey Nachman
IT Manager	Mr Dan Atkinson
Designated Safeguarding Lead	Mrs Kath Daniels
Data Protection Officer	Mrs Lesley Pye
e-Safety Governor	Mr Paul Archer

Table of Contents

Table of Contents 1
Introduction 4
1. Roles and Responsibilities 8
Governors 8
Senior Leadership Team 8
e-Safety Coordinator 9
IT Manager / ICT Services 9
Teaching and Support Staff 10
Designated Safeguarding Lead 11
Students 12
Parents and Carers 12
Supply Staff 13
2. Technology 13
3. Misuse 13
4. Email, Messaging and Social Networking 16
5. Use at Home 17
6. Personal Use 17
7. Privacy 18
8. Policy Violations 19
9. Responding to Incident of Misuse 20
10. Complaints 26
11. Filtering and Monitoring 26
Technology 26
Standards 27
Device Monitoring Standards 27
Appendices 29
Appendix 1 – Data Protection Act 2018 29
Appendix 2 - Email and Messaging – Good Practice Guide 30
Appendix 4 - Regulation of Investigatory Powers Act 2000 33
Appendix 5 – The General Data Protection Regulation 34
Appendix 6 – Relevant Legislation 35
Telecommunications (Lawful Business Practise) (Interception of communications) Regulations 2000 35

Contract law **35**
Copyright law **35**
Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988 ..... **35**
Computer Misuse Act 1990 ..... **35**
Appendix 7 - Lawful Business Practice Regulations (LBP) 35
Appendix 8 – Governors e-Safety Checklist 37
Appendix 9 – Flowchart for Responding to a Serious e-Safety Incident 39
Appendix 10 – Staff ICT Acceptable Use Policy No 44a 40
Computing Facilities **40**
Logging on and Security **40**
Use of the Network and Computer Facilities **41**
Use of the Internet **44**
Use of Email **45**
Social Media **46**
Use of Online/Distanced Learning programmes – Teams **46**
Personal Laptops / Computers / Devices **47**
Disciplinary Procedures **47**
ICT Services Helpdesk **47**
Mobile Device Encryption **47**
Remote Data Wipe **47**
Privacy and Personal Protection **47**
ICT Services **48**
Appendix 11 – Student ICT Acceptable Use Policy No. 44b 49
Computing Facilities **49**
Logging On and Security **49**
Use of the Network and Computer Facilities **49**
Use of the Internet **50**
Use of Email **52**
Use of Online/Distanced Learning programmes – Teams **52**
Personal Laptops / Computers / Devices **53**
Use of Other Technology **53**
Privacy and Personal Protection **53**
Disciplinary Procedures **54**

ICT Services **54**
Introduction and Context **55**
Professional Use of Social Media as an Educational Tool **56**
Personal Use of Social Media Advice for Employees **57**
Advice for other associates (including students) **58**
Using Social Media During School Hours **59**
Social Media in Lessons **59**
Policy Violations and Responding to Misuse **60**
What if I need to do something against this policy? **64**
Incident Reporting **64**
Appendix 14- General Advice for Online Safety and Responsible Use of Social Media 65
Appendix 15 – Advice for Staff for Online / Distances Teaching and Learning 68
Appendix 16 – Cyber Security Policy 71
Introduction **71**
Scope of Policy **71**
Risk Management **71**
Physical Security **71**
Asset Management **71**
User Accounts **71**
Devices **72**
Data Security **73**
Sharing Files **74**
Training **74**
System Security **74**
Major Incident Response Plan **75**
Maintaining Security **75**
Appendix 17 – Visitors Acceptable Use Policy 76
1. General Use **76**
2. Security and Privacy **76**
3. Prohibited Activities **76**
4. Monitoring and Compliance **76**
5. Device Support, Requirements, and Responsibility **76**

Introduction

This policy explains Colchester County High School for Girls (CCHSG) expectations of staff, students, and other users (working for or on behalf of Colchester County High School for Girls), in respect to the use of the Internet, e-mail, messaging systems and related technologies, including Buy Your Own Device (BYOD) laptops.

This policy applies to all Internet, email, messaging systems and all related technology services provided by Colchester County High School for Girls, and to all Colchester County High School for Girls users accessing these services. This guidance does not attempt to cover every situation but expresses the philosophy and general procedures users should apply when using any forms of ICT and electronic communication services at Colchester County High School for Girls.

The Internet, email, messaging systems and related technologies can be extremely valuable tools in an educational context, encouraging the development of communication skills, and transforming the learning process by opening possibilities that, conventionally, would be impossible to achieve. Colchester County High School for Girls encourage the use of electronic mail as a medium for paper mail replacement and as a means of enhancing communications.

Creating a safe ICT learning environment includes three main elements at Colchester County High School for Girls:

- An effective range of technological tools used to enhance teaching and learning, communication, and business systems.
- Policies and procedures, with clear roles and responsibilities.
- Access to e-Safety information for students, staff, parents and carers and other users.

Policy links:

- AT2 Alpha Trust Safeguarding & Child Protection Policy
- A4 Behaviour, Sanctions & Rewards Policy
- A5 Anti-bullying Policy
- 26 Code of Conduct
- 44a ICT AUP Policy - Student
- 44b ICT AUP Policy - Staff
- ICT Communications Procedures and Guidance for Staff (in Staff Handbook)
- 44c Social Media Policy
- 44d Generative Artificial Intelligence Policy

Please Note: This e-Safety Policy has been written by Colchester County High School for Girls e-Safety Coordinator, building on the Essex County Council Model Policy, the London Grid for Learning (LGfL) model policy and the Southwest Grid for Learning SWGfL model policy. It has been agreed by Colchester County High School for Girls Local Governing Body, Senior Leadership Team, IT Manager, and the e-Safety Coordinator.

Context Including Online Safety and Filtering and Monitoring

Harnessing Technology: Transforming learning and children's services [1] sets out the government plans for taking a strategic approach to the future development of ICT.

"The Internet and related technologies are powerful tools, which open new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.
To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom."

Statutory guidance including the provisions of the *Children Act 2004*[2], and *Keeping Children Safe in Education*[3] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- Safe from maltreatment, neglect, violence, and sexual exploitation.
- Safe from accidental injury and death.
- Safe from bullying and discrimination.
- Safe from crime and anti-social behaviour in and out of school.
- Secure, stable, and cared for.

Much of these aims apply equally to the 'virtual world' that students will encounter whenever they use ICT in its various forms, including Artificial Intelligence. For example, we know that the Internet has been used for grooming young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or social media messages; and we know that students have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of Colchester County High School for Girls to ensure that every student in their care is safe, and the same principles should apply to the 'virtual' or digital world as are applied to Colchester County High School for Girls physical buildings.

[1] www.dfes.gov.uk/publications/e-strategy

[2] www.education.gov.uk/publications

[3] Keeping Children Safe in Education, DfE, 2024

This Policy document is necessary to protect all parties and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Online Safety

We recognise that our students are growing up in an increasingly complex world, living their lives on and offline. Whilst this presents many positive and exciting opportunities, we recognise it also presents challenges and risks, in the form of:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: 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: online behaviour that increases the likelihood of, or causes, harm; for example, 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.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial frauds.

Filtering & Monitoring

Filtering

Filtering software is used on the school network to prevent access to inappropriate internet sites, and to protect the computer systems. To ensure students are safeguarded from potential harmful and inappropriate online material, including online radicalisation (PREVENT), our filtering system manages the below table of content.

Online filtering involves using software or hardware tools to control and restrict access to harmful or inappropriate websites and content categories. This can include URL, keyword, or category-based filtering to help shield children from harmful material such as adult content, violence, drugs, Extremism* and hate speech.

Below is a table of the currently blocked core categories of which no user can access:

Discrimination	Content that promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010
Drugs / Substance abuse	Content that displays or promotes the illegal use of drugs or substances
Extremism*	Extremism is the promotion or advancement of an ideology based on violence, hatred or intolerance that aims to: 1. negate or destroy the fundamental rights and freedoms of others; or 2. undermine, overturn or replace the UK's system of liberal parliamentary democracy and democratic rights; or 3. intentionally create a permissive environment for others to achieve the results in (1) or (2). (Gov.UK definition of extremism 2024)
Gambling	Content that enables gambling
Malware / Hacking	Content that promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
Pornography	Content that displays sexual acts or explicit images including audio, visual or text
Piracy and copyright theft	Content that includes illegal provision of copyrighted material for illegal download or streaming
Self-Harm	Content that promotes or displays deliberate self-harm (including suicide and eating disorders)
Violence	Content that displays or promotes violence
Child Abuse	Content that contains keywords relating to child abuse provides by the IWF
Gore	Sites displaying or describing gory content
Naturism and Nudism	Sites that contain nudist pictures
Restricted to adults	Sites containing the "Restricted to Adults" special tag.
Custom Blocked content	Any website URLs added to this category based on assessment of suitability.

Monitoring

Online monitoring is about observing and tracking our school community's digital activities, including web browsing, social media interactions and chat conversations. It aims to identify potential risks, rule violations, and raise alerts that can be acted on. Monitoring helps encourage students to become good digital citizens.

1. Roles and Responsibilities

This section is intended to outline who takes responsibility for each element of e-Safety, the acceptable use of the Internet, e-mail, messaging systems and related technologies in the school.

Governors

The school's governing body are responsible for the approval of the policies contained within this document and for reviewing their appropriateness. A member of the governing body has the role of e-Safety Governor.

This role includes:

- Annual or more regular meetings with the e-Safety Coordinator to complete the Governors e-Safety Checklist (see Appendix 8)
- Monitoring of the schools e-Safety Incident Logs (CPOMS)
- Monitoring of the filtering and permissions procedures
- Reviewing the Annual Audit to ensure compliance with KCSIE requirements for Online Safety and Filtering and Monitoring
- Reporting to the governing body

Senior Leadership Team

- In-line with the schools safeguarding policy the Principal* assumes overall responsibility for the safety, including e-Safety, of all members of the school community, though the day-to-day enforcement of e-Safety, appropriate use of the schools ICT systems and appropriate internet conduct will be delegated to the IT Manager. Safeguarding issues that arise out of e-Safety incident will be delegated to the Designated Safeguarding Lead. The e-Safety Coordinator will be advised as appropriate.
- The Senior Leadership Team are responsible for ensuring that the relevant personnel outlined in this section are given adequate support and relevant CPD to allow them to carry out their role effectively and where necessary train others.
- The Senior Leadership Team are responsible for ensuring that appropriate training is provided to allow staff to understand the need for and the ability to follow the procedures outlined in these policies.
- The Principal* and Senior Leadership Team must be made aware of the protocol following a serious incident concerning e-Safety, Online Safety, misuse of ICT or inappropriate internet conduct.
- In the event of a serious incident the Executive Principal must be fully informed and given the opportunity to decide how the incident be managed.

***Please note:**

The term "Principal" is used at Colchester County High School for Girls to identify the person with responsibilities of headship, who may be referred to locally as Executive Headteacher or Associate Principal

e-Safety Coordinator

The e-Safety coordinator is responsible for:

- Reporting wider incidents concerning e-Safety (i.e. Tik Tok trends), to the Designated Safeguarding Lead and other relevant personnel.
- Liaise with Year Leaders who take day to day responsibility for e-Safety, misuse of ICT or inappropriate internet conduct issues. The e-Safety Coordinator has a leading role in educating students those who need extra guidance and advice.
- Contributes to the reviewing the school policy document.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-Safety, Online Safety, misuse of ICT or inappropriate internet conduct incident taking place.
- Providing adequate training and advice for staff that will allow them to understand the need for and the ability to follow the procedures outlined in these policies.
- Providing appropriate information and training for parents/carers regarding e-Safety, appropriate use of ICT and internet conduct
- Ensuring there is adequate provision for e-Safety and appropriate internet use in the computing curriculum.
- Liaising with appropriate governing bodies and the e-Safety Link Governor
- Liaises with the Designated Safeguarding Lead and views logs of incidents using the CPOMS to inform future e-Safety developments.
- Meeting regularly with e-Safety Governor to complete the Governors e-Safety Checklist, discuss current issues and review incident logs.
- Attending relevant meetings and training with regard to e-Safety.

IT Manager / ICT Services

IT Manager and the ICT Services Department are responsible for ensuring:

- That the school's ICT infrastructure, including the filtering and monitoring software is secure and is not open to misuse or malicious attack.
- That the network infrastructure meets the needs of the school and provides all users with the ability to follow the procedures outlined within these policies
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are continually changed.
- The school's filtering of internet content to individual groups is appropriate and in line with government policy and the Internet Service Provider Recommendations
- That they keep up to date with appropriate technical information to effectively carry out their e-Safety role and to inform and update others as relevant
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the e-Safety Coordinator and Principal for investigation / action /sanction.
- Web filter will continue to monitor web browsing for all users.

- Ensuring that the relevant filtering and monitoring solutions are tested and confirmed working and meeting compliance against the KCSIE requirements.

Teaching and Support Staff

All members of teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of e-Safety, KCSIE, PREVENT and internet conduct matters and of the policies outlined in this document.
- They have read, understood, and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- They report any suspected e-Safety incident, misuse or inappropriate internet conduct to the Designated Safeguard Lead or Deputy Designated Safeguard Lead by completing an orange safeguarding form. This will be logged by the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead on CPOMS. The e-Safety Coordinator and IT Manager will be informed of any serious incidents which are for investigation /action /sanction by the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead.
- They report any suspected e-Safety incident, misuse or inappropriate internet conduct to the e-Safety Coordinator and IT Manager for investigation, action or sanction.
- Digital communications with students and staff via email or via any other method should be on a professional level and only carried out using official school systems and are in line with the school Code of Conduct
- e-Safety, appropriate use of ICT systems and equipment, and internet conduct issues are embedded in all aspects of the curriculum and other school activities.
- They monitor the use of school managed and internet activity in lessons, extracurricular and extended school activities using the supplied monitoring software used within the corporate network and applying the monitoring standards detailed in this document.
- Students understand and follow the aspects of the policies outlined in this document that are relevant to them.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They are aware of e-Safety issues related to the use of mobile phones, cameras, and hand-held devices and that they monitor their use and implement current school policies regarding these devices.
- In lessons where internet use is pre-planned students should be guided to sites that have been checked as suitable for their use and should any inappropriate content be discovered because of an internet search this is reported to the e-Safety Coordinator and ICT Services
- Should the lesson contain content that could be related to any blocked content or content that could be flagged as a safeguarding issue, the Designated Safeguarding Lead should be notified in advanced of the lesson to pre-empt any alerts that could be generated.

Designated Safeguarding Lead

The Designated Safeguarding Lead and Deputies should be trained in e-Safety and internet conduct/cyber-bullying issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- On-line contact with adults /strangers
- Potential or actual incidents of grooming and child exploitation including online sexual and financial exploitation.
- Cyber-bullying

All Staff have a duty to report failings in technical safeguards which may become apparent when using systems and services. You should report if:

- You witness or suspect unsuitable material has been accessed.
- You can access unsuitable material.
- You are teaching topics which could create unusual activity on the filtering logs.
- There is a failure in the software or abuse of the system.
- There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks.
- You notice abbreviations or misspellings that allow access to restricted material.

The Designated Safeguarding Lead assumes primary responsibility for safeguarding and online safety, which includes overseeing and responding to:

- Filtering and monitoring reports
- Safeguarding concerns
- Checks on filtering and monitoring systems on different devices around the school and different users

The Designated Safeguarding Lead and Deputies should be trained in e-Safety and internet conduct/cyber-bullying issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials, including those deemed to be Extremist materials
- On-line contact with adults /strangers
- Potential or actual incidents of grooming and child exploitation including online sexual and financial exploitation.
- Cyber-bullying

Students

Students are responsible for:

- Using the school ICT systems in accordance with the Students Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Understanding and following the aspects of the policies outlined in this document that are relevant to them.
- Having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Understanding and following the procedures outlined in the school policies on the use of mobile devices, digital cameras, and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-Safety practice and internet conduct when using digital technologies out of school and realise that the school's e-Safety, ICT Acceptable Use, and Internet Code of Conduct Policy covers their actions out of school, if related to their membership of the school

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of modern technology than their children. The school will therefore take every opportunity to help parents understand these issues through Parent Information Evenings, newsletters, letters, the school website, and information about national/local e-Safety campaigns. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy
- providing adequate support to allow their child to operate within the procedures outlined in these policies.
- Supporting the school by providing any relevant information regarding their child's online activity/access in the event of an incident
- Monitoring their child's use of the internet and online activity using mobile devices at home
- Giving specific permission for their child to participate in the live streaming of lessons.

Supply Staff
Supply staff will be requested to read and sign the Staff Acceptable Use Policy. They will be expected to follow the procedures outlined in these policies that are appropriate to their role in the school.

Visitors
Visitors will be required to read the Visitors Acceptable Use Policy before acknowledging this on InVentry on sign in. They will be expected to follow the guidance set in this AUP for their time within the organisation.

2. Technology
ICT in the 21st Century has an all-encompassing role within the lives of students and adults. Modern technologies are enhancing communication and the generation and sharing of information. Current and emerging technologies used at Colchester County High School for Girls and, more importantly in many cases, used outside of Colchester County High School for Girls by students (and staff) include but are not limited to:

- The Internet
- E-mail
- Instant messaging often using simple web cams e.*g. Facebook Messenger, Skype, WhatsApp*
- Online / distanced learning platforms like Microsoft Teams
- The use of school approved AI platforms (e.g. Microsoft copilot/ SLT AI)
- Blogs / vlogs (an on-line interactive diary) e.g. *Bloggers*
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player).
- Social networking sites e.g. *Facebook, X (formally known as Twitter), Instagram, Tumblr*
- Video broadcasting and streaming sites e.g. *YouTube, iPlayer, Netflix* chat rooms e.g. *Snapchat, Kids-online, Penguinchat, Habbo-Hotel*
- Gaming sites e.g. *Mini-clip, Addicting games,* and gaming platforms like Discord
- Music and book download sites e.g. *iTunes, Amazon, Google Play, Napstar*
- Mobile phones with, Bluetooth, messaging, camera, and video functionality; smart watches with Bluetooth and messaging functionality
- Messaging or Bluetooth communications between systems and mobile devices.
- Smart phones with e-mail, web functionality and cut down ‘Office’ applications.
- Mobile devices that access the Internet both inside and outside of Colchester County High School for Girls premises.
- Remote access to Colchester County High School for Girls recourses (including via BYOD)
- School provided systems such as Office 365

3. Misuse
The Internet, email, any other online messaging systems, and related technologies must not be used for knowingly viewing, transmitting, retrieving, downloading, or storing any communication that is:

- Discriminatory, harassing, or derogatory to any individual or group
- Obscene or pornographic, or deemed to be obscene or pornographic.
- Defamatory, threatening or seen as cyber-bullying.
- Illegal or contrary to Colchester County High School for Girls policy or interests
- Subject to Copyright such as music, software, or films
- Likely to cause network congestion or significantly hamper access for other users.
- Any of the above, specifically using mobile devices or similar technologies to store or upload any such materials to the public domain (social-media sites) or to other devices.

Except in cases in which explicit authorisation has been granted by Colchester County High School for Girls Senior Leadership Team, users are prohibited from engaging in, or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other users.
- Using other user's logins or passwords
- Sending or checking emails during lesson time, including email conversations with colleagues that could be deemed of a personal nature.
- Breaching, testing, or monitoring computer or network security measures.
- E-mail or other electronic communication that attempts to hide the identity of the sender or represent the sender as someone else.
- Hacking, Blue-jacking, or accessing systems or accounts that they are not authorised to use.
- Obtaining electronic access to other companies' or individuals' materials. (Copyright means users cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner).

The Law and Colchester County High School for Girls Policy prohibit the theft or abuse of computing resources and includes:

- Unauthorised entry
- Using, transferring, and tampering with other people's accounts and files
- Interfering with other people's work or computing facilities
- Sending, storing, or printing offensive or obscene material including content that may be interpreted as sexual or racial harassment.
- Mass mailing of messages
- Internet use for personal or commercial purposes
- Using the internet facilities or equipment to deliberately propagate any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations.
- Accessing or uploading to any obscene, pornographic or any site of a sexual nature. Sexually explicit material may not be viewed, archived, generated, stored, distributed, edited, emailed, or recorded using the school's networks or computing resources.

If a user finds themselves connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately. Such unintentional access to inappropriate internet sites must be reported immediately to the e-Safety Coordinator, Senior Leadership Team, IT Manager or Principal. Any failure to report such access may result in disciplinary action as per the school Code of Conduct.
It is impossible to define all possible unauthorised use, however, disciplinary action may be taken where a user's actions warrant it. Other actions deemed unacceptable, although not exhaustive, include:

- Users shall not visit Internet sites, generate, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals, or comments that contain or relate to:
    - Child sexual abuse images
    - Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation.
    - Adult material that potentially breaches the Obscene Publications Act in the UK or could be deemed as inappropriate in a school setting.
    - Promotion of any kind of discrimination
    - Promotion of racial, religious, or political hatred
    - Promotion of terrorist activity, whether current or historical
    - Threatening behaviour, including promotion of physical violence or mental harm
    - Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.
- Running a personal business during school hours or with school equipment
- Use systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Uploading, downloading, or transmitting to the school system any commercial software or copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising online confidential or proprietary information relating to the school (e.g. financial / personal information, databases, computer/network access codes and passwords)
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet.
- Accessing pornographic material or material deemed inappropriate to a school setting during school hours or using school equipment Using personal devices to record students or their work for purposes not deemed educational or outside the remit of the classroom and without permission from the Senior Leadership Team
- Forward any form of chain email.
- Using school messaging systems especially email to conduct personal communication not deemed school business or for educational purposes or

- Gambling online during school hours or using school equipment and noneducational online gaming during directed time.
- Posting with location based social-media platforms during school hours or whilst on the school premises i.e. checking in with Facebook or similar sites.
- Using file sharing systems during school hours or with school equipment
- Using online accounts during school hours for personal (non-educational) reasons, this includes but is not limited to email, social-media platforms, online banking, blogging, live-casting.
- Using e-commerce to shop online during school hours including app and media purchases.
- Streaming non-educational video or audio content during directed work/learning hours
- Theft or copying of files without permission.
- Sending or posting Colchester County High School for Girls or local authority's confidential files outside of the organisation or inside the organisation to unauthorised staff, students, or other users
- Refusing to co-operate with a reasonable security investigation

4. Email, Messaging and Social Networking

Those that use Colchester County High School for Girls e-mail, messaging or other digital communication services are expected to do so responsibly, comply with all applicable laws, policies, and procedures of Colchester County High School for Girls, and with normal standards of professional and personal courtesy and conduct. See Appendix 2 for an illustration of good practice.

The school follows sound professional practices to secure e-mail records, messaging systems, data, and system programmes under its control. As with standard paper-based mail systems, confidentiality of these cannot be 100% assured. Consequently, users should consider the risks when transmitting highly confidential or sensitive information and use the appropriate level of security measure.

To effectively manage these systems, the following should be adhered to:

- Devices not to be left unlocked when unattended.
- Mailboxes should never be visible to a class or the public.
- Inboxes should be kept organised with old messages deleted and important messages that require preserving saved to appropriate folders.
- Care should be taken about the content of a message as it has the same standing as a letter. Report immediately to ICT support when a virus is suspected in a message.

Users must not:

- Ignore messages. These systems are designed for concise communication. If the message requires a reply, a response should be sent promptly but not during lessons, as per the school Code of Conduct

- Use anonymous messaging services to conceal identity when mailing through the Internet (except for the use of Whisper); falsify e-mails to make them appear to originate from someone else or provide false information to any Internet service which requests name, e-mail address or other details.
- Abuse others, either in joke (banter) or in response to abuse directed at them or use inappropriate language or images in communication with others.
- Use these technologies, either internally or on the Internet, to harass (sexually or otherwise) fellow employees, or harass or threaten anyone in any manner.

The transmission of usernames, passwords, chain mail or other information related to the security of Colchester County High School for Girls computers is not permitted.

5. Use at Home

Students, staff, or other users accessing the Internet from home whilst using a Colchester County High School for Girls owned device or accessing data through personal devices on SharePoint or other services must adhere to the policies set out in this document and adhere to the school Code of Conduct.

Family members or other non-Colchester County High School for Girls users must not be allowed to access the school's computer system or use the school's computer facilities, without the formal agreement of the Senior Leadership Team.

6. Personal Use

The Internet, e-mail, messaging systems and other related technologies are business tools provided to users at significant cost. Hence, it is expected that this resource will be used for professional/educational related purposes. Reasonable access and use of these systems is also available to recognised representatives of professional associations i.e. Union Officers.

These systems may be used for incidental personal purposes, with the approval of the Senior Leadership Team / e-Safety Coordinator, if it does not:

- Contravene the statements laid out in the Misuse section.
- Interfere with Colchester County High School for Girls operation of computing facilities or e-mail services.
- Interfere with the user's employment or other obligations to Colchester County High School for Girls
- Interfere with the performance of professional duties, including the delivery of lessons and preparation of learning materials.
- Is of a limited duration and frequency
- Is performed in non-work time.
- Does not over burden the system or create any additional expense to Colchester County High School for Girls.

Such use must not be for:

- Any action which does not safeguard students at Colchester County High School for Girls
- Unlawful activities
- Commercial purposes not under the auspices of Colchester County High School for Girls
- Personal financial gain
- Personal use inconsistent with other Colchester County High School for Girls policies or guidelines.

All such use should be done in a manner that does not negatively affect the use of Colchester County High School for Girls systems for professional / educational purposes. Users are expected to demonstrate a sense of responsibility and not abuse this privilege.

7. Privacy

Colchester County High School for Girls respects users' privacy, e-mail content will not be routinely inspected or monitored, nor content disclosed without the originator's consent. However, under the following circumstances such action may be required:

- When required by law.
- If there is a substantiated reason to believe that a breach of the law or Colchester County High School for Girls e-Safety Policy/Code of Conduct has taken place
- If there is a substantiated reason to believe that a breach of Safeguarding has taken place
- When there are emergency or compelling circumstances

Colchester County High School for Girls reserves the right, at its discretion, to review any user's electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy, and other Colchester County High School for Girls policies.

Users should not have any expectation of privacy to their internet usage or any activity taking place on a school managed device or whilst signed into the schools Wi-Fi. Colchester County High School for Girls reserves the right to inspect all files on any corporate location including OneDrive and SharePoint to assure compliance with this policy. Auditors must be given the right of access to any document, information, or explanation that they require.

The use of students, staff or other users designated personal file area[4] on the network server provides some level of privacy in that it is not readily accessible by

[4] Before storing confidential information in this way, users are advised to ensure that they understand how to save information to their personal file area. Please also ensure GDPR guidance and policy is being followed when storing identifiable information.

other users. These file areas will however be monitored to ensure adherence to Colchester County High School for Girls policies and to the law. The user's personal file area (N: Drive / OneDrive for business) is located on cloud storage and is allocated to that user.

Managers will not routinely have access to a user's personal file area. However, usage statistics / management information on usage size of drives or a report outlining the amount of information held on an individual's personal file area will be made available from time to time or on request.

8. Policy Violations

Staff, students or other users who abuse the privilege of Colchester County High School for Girls facilitated access to the Internet, e-mail, messaging systems or other related technologies face being subjected to disciplinary action, up to and including termination of employment (staff) or suspension / permanent exclusion (students), and risk having these privilege removed for themselves and possibly other employees / peers.

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the actions that will be taken against misuse.

If any apparent or actual misuse involves illegal activity i.e.

- Child sexual abuse images
- Adult material which is inappropriate for a school setting or potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity, or materials.

The flow chart (Appendix 9) should be consulted, and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence, and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Incidents of student misuse will be addressed using the school Student Behaviour, Sanctions and Rewards Policy and procedures and reported to the parents, e-Safety Coordinator, Senior Leadership Team and when necessary, the Principal and e-Safety Governor.

Incidents of Staff / Volunteer misuse will be addressed using the Staff Disciplinary Procedures and reported to line manager, Senior Leadership Team, Executive Principal and when necessary, the e-Safety Governor and Governing Body.

9. Responding to Incident of Misuse

An online safety concern or e-Safety incident should be acted upon promptly to allow the situation to be investigated and necessary personnel, which is likely to include parents and the police to be informed in a timely fashion.

Any incidents where students do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures / the guidance outlined in the AUP or as detailed below.

In situations where a member of staff is made aware of a serious e-Safety incident that concerns students or staff, they should follow the schools Safeguarding reporting procedures and report the incident fully on an Orange Safeguarding form. This Orange form should be passed immediately to the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead in person. This incident will then be recorded on CPOMS as a specific e-Safety incident and the e-Safety Coordinator will be informed. If the child is at immediate risk of harm, the Designated Safeguarding Lead or Deputy Designated Safeguarding Leads will follow the procedures outlined in A3 Child Protection Procedures (section 5 and 6)

Instances of cyberbullying will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognises that staff as well as students may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's e-Safety Coordinator and IT Manager and appropriate advice sought, and action taken to minimise the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy, then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that student data has been lost.

School reserves the right to utilise filtering and monitoring software on their premises and to search any technology equipment, including personal equipment, with permission, when a breach of this policy is suspected.

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the school's Safeguarding Policy will be followed.

The following should be used as guidance on acting and applying sanctions following an e-Safety incident.

Student Sanctions:

Incident/Misuse	Refer to class teacher/form tutor.	Refer to Pastoral Leader	Refer to Senior Leadership (DSL)	Refer to the Principal.	Refer to the Police.	Refer to IT Manager or ICT Services	Inform parents/carers.	Removal of internet access rights	Warning	Detention	Further consequence e.g. exclusion
Deliberately accessing or trying to access material that could be considered illegal		x	x	x	x	x	x	x	x	x	x
Unauthorised use of noneducational sites during lessons	x	x				x	x	x	x	x	
Unauthorised use of mobile phone/digital camera/another handheld device	x	x					x		x	x	
Unauthorised use of social networking/ instant messaging/personal email	x	x				x	x	x	x	x	
Unauthorised downloading or uploading of files	x	x				x	x	x	x	x	
Allowing others to access school network by sharing username and passwords	x	x				x	x	x	x	x	
Attempting to access or accessing the school network,	x	x				x	x	x	x	x	

Incident/Misuse	Refer to class teacher/form tutor.	Refer to Pastoral Leader	Refer to Senior Leadership (DSL)	Refer to the Principal.	Refer to the Police.	Refer to IT Manager or ICT Services	Inform parents/carers.	Removal of internet access rights	Warning	Detention	Further consequence e.g. exclusion
using another student's account											
Attempting to access or accessing the school network, using the account of a member of staff		x	x			x	x	x	x	x	
Corrupting or destroying the data of other users		x	x			x	x	x	x	x	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x	x	x	x	x	x	x	x	x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	x	x		x	x	x	x	x	x
Using proxy sites or other means to subvert the school's filtering system		x	x	x		x	x	x	x	x	
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x			x	x	x		x		
Deliberately accessing or trying to access offensive or pornographic material	x	x	x		x	x	x	x	x	x	

Incident/Misuse	Refer to class teacher/form tutor.	Refer to Pastoral Leader	Refer to Senior Leadership (DSL)	Refer to the Principal.	Refer to the Police.	Refer to IT Manager or ICT Services	Inform parents/carers.	Removal of internet access rights	Warning	Detention	Further consequence e.g. exclusion
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		x	x			x	x		x		
Intentionally removing or bypassing monitoring software installed.	x	x	x			x					
Intentionally testing or misusing the monitoring software.	x	x	x			x					
Intentionally damaging the computing equipment	x	x	x	x	x	x	x	x	x	x	x

Staff Sanctions

Incident/misuse	Refer to Line manager.	Refer to Designated Safeguarding Lead (DSL).	Refer to Local Authority, HR, and LADO.	Refer to the Police.	Refer to IT Manager or ICT Services	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal	x	x	x	x	x	x	x	x
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	x	x			x	x		
Unauthorised downloading or uploading of files	x	x			x	x		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's Account	x	x			x	x		
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x			x	x		
Deliberate actions to breach data protection or network security rules	x	x			x	x	x	x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x			x	x	x	x
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x	x		x	x	x	x	x

Incident/misuse	Refer to Line manager.	Refer to Designated Safeguarding Lead (DSL).	Refer to Local Authority, HR, and LADO.	Refer to the Police.	Refer to IT Manager or ICT Services	Warning	Suspension	Disciplinary action
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students	x	x		x	x	x	x	x
Actions which could compromise the staff member's professional standing	x	x	x		x	x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x	x		x	x	x	x
Using proxy sites or other means to subvert the school's filtering system	x	x			x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x		x	x	x		
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x
Breaching copyright or licensing regulations	x	x			x	x		
Continued infringements of the above, following previous warnings or sanctions	x	x	x	x	x	x	x	x
Intentionally removing or bypassing monitoring software installed.	x	x			x			
Intentionally testing or misusing the monitoring software.	x	x	x		x			
Intentionally damaging the computing equipment	x			x	x	x	x	x

10. Complaints

Colchester County High School for Girls will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a Colchester County High School for Girls computer or mobile device. Neither Colchester County High School for Girls nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Students and staff have access to information about infringements in use and sanctions.

Sanctions available include:

- Interview or counselling by Form Tutor/Year Leader /e-Safety Coordinator/ Senior Leadership Team
- Informing parents or carers of students
- Removal of Internet or computer access for a period, which could prevent access to files held on the system, including staff files or student examination coursework.
- Referral to Local Authority and / or Police.

The e-Safety Coordinator acts as first point of contact for any complaint. However, any complaint about staff must also be referred to either of the Associate Principals.

Complaints of Cyber-bullying is dealt with in accordance with the Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the Safeguarding Policy and reference to SET Procedures.

11. Filtering and Monitoring

Technology

The technology in use within the organisation allows for granular control, reporting and alerting for all services surrounding filtering and monitoring.

Online filtering involves using software or hardware tools to control and restrict access to harmful or inappropriate websites and content categories. This can include URL, keyword, or category-based filtering to help shield children from harmful material such as adult content, violence, drugs, Extremism and hate speech.

Online monitoring is about observing and tracking our school community's digital activities, including web browsing, social media interactions and chat conversations. It aims to identify potential risks, rule violations, and raise alerts that can be acted on. (see P32 for the monitoring table).

Colchester County High School for Girls approach to filtering and monitoring is in line with the Keeping Children Safe in Education requirements, including those for PREVENT. We use technology available to us to be able to effectively filter, safeguard and monitor devices without this impacting on education. We do not over block and restrict to an extent where web browsing and research opportunities are not possible. Any websites that are being blocked can be requested to be unblocked, ICT Services will complete a risk assessment to see if the site is suitable for student / staff consumption.

All devices have software installed which allows for remote monitoring. This monitoring software tracks keystrokes and takes screenshots of potential safeguarding issues or inappropriate activity. The current software in use will then pass this up to an artificial intelligence model which will assess if there is any risk associated with the activity. If there is a risk of one of the core categories we protect against, for example self-harm, then this will be passed to a human moderator who will grade the alert from 1-5. Five being the most serious and requiring immediate intervention. This software is always active and will send alerts when connected to the internet. This software cannot be used for covert monitoring by any staff. This function is not built into the software. Any remote control of any device is completed through ICT Services. Any user will know if a device is being controlled / viewed by the Team Viewer box in the bottom right corner of the screen showing the agent's name current controlling.

Standards

As detailed in the Keeping Children Safe in Education (2024), we aim to meet the four standards set. In this document, we have identified named roles and responsibilities for staff to manage the filtering and monitoring. We audit our filtering and monitoring provision annually and review if our supplier is meeting the needs of the organisation. Our filtering and monitoring solutions block harmful content without unreasonably impacting teaching and learning. A team of designated people, usually the IT Manager, Designated Safeguarding Lead, e-Safety lead, and members of Senior Leadership Team, meet half termly to discuss and review the current state of filtering and monitoring and to review if any significant changes are needed. We have an effective monitoring strategy in place which allows for safeguarding alerts to be automatically sent to the appropriate named personnel. Any safeguarding alerts from either web browsing or monitoring are sent to the respective year leader / Designated Safeguarding Lead. Automated reports on the week's events are also sent weekly.

Device Monitoring Standards

There are four monitoring strategies that are in use within the organisation.
As a standard, all corporate devices have individual device monitoring through software and third-party services, this is the SmoothWall Monitor.
All corporate devices have network Monitoring using log files of internet and web traffic using the SmoothWall Cloud browser extensions.

In the case of personal devices, these are authenticated against the web filter to be able to identify the user. All web traffic is then associated against that user to allow for the story to be built of what the student was browsing on that device. There is currently no software solution available to be able to monitor or live view personal owned devices. Personal devices are to be monitored on web traffic only.
Both strategies have user identifiable information and screen shots if applicable. This is the default standard we accept within the organization and is a catch all approach as all corporate devices has this to meet the monitoring requirements of the KCSIE.
Building upon the default, staff are also able to live view their class who are logged onto corporate devices from the “Teacher” station or laptop using SmoothWall Classwize. This software allows the member of staff to be able to live view the screen of the students in their class, able to send URLs to the devices, able to block internet and restrict web browsing to specific sites. This allows the members of staff to ensure their class is on track and able to monitor live what their students are doing. As a last resort, staff will physically monitor the devices in use by walking around the classroom. This is the least preferred method as the other methods have the technology to see behind what is being displayed behind the open window.

Appendices

Appendix 1 – Data Protection Act 2018

The General Data Protection Regulation prohibits the disclosure of personal data except in accordance with the principles of the Act. This prohibition applies to email in the same way as to other media. Information gathered on the basis that it would be seen by specified employees must not be given to a wider audience. In accordance with the provisions of Article 8 of the European Convention on Human Rights[5], the School respects the right to privacy for employees who use IT equipment but does not offer any guarantee of privacy to employees using IT equipment for private purposes.

As data controller, Colchester County High School for Girls has responsibility for any data processed or stored on any of its equipment. Any employee monitoring will be carried out in accordance with the principles contained in the Code of Practice issued by the Information Commissioner under the provisions of the Data Protection Act 2018.

In order to comply with its duties under the Human Rights Act 1998, Colchester County High School for Girls is required to show that it has acted proportionately, i.e. are not going beyond what is necessary to deal with the abuse and that the need to investigate outweighs the individual's rights to privacy, taking into account the schools wider business interests. In drawing up and operating this policy the school recognises that the need for any monitoring must be reasonable and proportionate.

Auditors (internal or external) are able to monitor the use of Colchester County High School for Girls IT equipment and the storage of data. They are nevertheless bound by the provisions of the Human Rights Act 1998, the Data Protection Act 1998, associated codes of practice and other statutory provisions and guidance, including the Regulation of Investigatory Powers Act 2000 in respect of any activity that could be classed as directed surveillance[6]. (See Appendix 2)

5 Everyone has the right to respect for his private and family life, his home, and his correspondence.

6 [6] Directed Surveillance' is defined as surveillance which is covert (i.e. carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place) but not intrusive, for the purpose of a specific investigation in such a manner as is likely to result in the obtaining of private information about a person.

Appendix 2 - Email and Messaging – Good Practice Guide

	Good Practice
Read Receipt	When it is important to know that a recipient has opened a message, it is recommended that the sender invoke the 'read receipt' option.
Attachment Formats	When attaching a file, it will have a specific format. Be aware of the possibility that a recipient may not have the software necessary to read the attachment. Format incompatibility can occur even between successive versions of the same software, e.g. different version of Microsoft Word.
Email Address Groups	If messages are regularly sent to the same group of people, the addressing process can be speeded up by the creation of a personal group in the personal address book.
Message header, or subject	Convey as much information as possible within the size limitation. This will help those who get a lot of emails to decide which are most important, or to spot one they are waiting for.
Subject	Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to archive.
Recipients	Beware of sending messages to too many recipients at once. When sending messages for more than one-person's use be sure to indicate people for whom there is some expectation of action or who have central interest; cc to indicate those who have peripheral interest and who are not expected to act or respond unless they wish to do so.
Replying	When replying to a message sent to more than one person, do not routinely reply to all recipients of the original message. Consider who needs to read your reply, e.g. if the sender is organising a meeting and asking you for availability dates, you need only reply to the sender.
Absent	If you have your own Email address, it is possible, for users of MS Exchange or have local enhancements to MS-mail, to set the 'out of office' message when you are going to be away for some time, e.g. on annual leave. You will not lose your messages, they will await your return, but the sender will know that you are not there and can take alternative action if necessary.

	Good Practice
Evidential Record	Never forget that electronic conversations can produce an evidential record which is absent in a telephone conversation. Comments made by an employee during an exchange of emails could be used in support, or in defence, of the Academy's legal position in the event of a dispute.
Legal records	Computer generated information can now be used in evidence in the courts. Conversations conducted over the Email can result in legally binding contracts being put into place.
Distribution Lists	Keep personal distribution lists up-to-date and ensure you remove individuals from lists that no longer apply to them.
Email threads	Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is best that a response to a message is continued by using reply accessed on the quick menu bar, rather than start an entirely new message for a response. Keep the thread information together. It is easier for the participants to follow the chain of information already exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message.
Context	Email in the right context, care should be taken to use Email where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of the use of excessive use of capitals. It can be interpreted as SHOUTING so consider how the style of your email may be interpreted by its recipient.
Forwarding Emails	Consideration should be given when forwarding Emails that it may contain information that you should consult with the originator before passing to someone else.
Large Emails	For larger Emails, particularly Internet Emails, where possible send at the end of the day as they may cause queues to form and slow other people's Email.

Appendix 3 - Legislative Framework - The Human Rights Act 1998

This provides for the concept of privacy, giving a ‘right to respect for private and family life, home and correspondence.’ The provision is directly enforceable against public sector employers, and all courts must now interpret existing legislation in relation to the Human Rights Act. Halford v UK 1997 suggests that employees have a reasonable expectation of privacy in the workplace, and employers are recommended to provide workers with some means of making personal communications which are not subject to monitoring, for instance a staff telephone line or a system of sending private Emails which will not be monitored.

Covert monitoring is likely to be unlawful unless undertaken for specific reasons as set out in the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (see below). Employers should make sure workers know of any monitoring or recording of correspondence (which includes Emails, use of Internet, telephone calls and faxes etc.).

Appendix 4 - Regulation of Investigatory Powers Act 2000

This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system and applies to public and private communication networks. It gives the sender or recipient of a communication the right of action for damages against the employer for the unlawful interception of communications.

There are two areas where monitoring is not unlawful. These are:

- Where the employer reasonably believes that the sender and intended recipient have consented to the interception

- Without consent, the employer may monitor in the following circumstances, as set out in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. These include:

- to ensure compliance with regulatory practices
- to ensure standards of service are maintained, e.g. in call centres.
- to prevent or detect crime.
- to protect the communications system this includes unauthorised use and potential viruses.
- to determine the relevance of the communication to the employer's business i.e. picking up relevant messages when someone is away from work.

However, the employer is expected to make all reasonable efforts to ensure system users know that communications may be intercepted, and any such monitoring must also comply with the provisions of the Data Protection Act 1998 (see below), and in particular the Data Protection principles on fair processing.

Appendix 5 – The General Data Protection Regulation

The Information Commissioner - responsible for enforcement of the General Data Protection Regulation - is publishing four codes of practice to help employers comply with the provisions of the Data Protection Act. These codes clarify the Act in relation to processing of individual data, and the basis for monitoring and retention of email communications.

The code of practice '*Monitoring at work: an employer's guide*' states that any monitoring of emails should only be undertaken where:

- The advantage to the business outweighs the intrusion into the workers' affairs - Employers carry out an impact assessment of the risk they are trying to avert workers are told they are being monitored.
- Information discovered through monitoring is only used for the purpose for which the monitoring was carried out.
- The information discovered is kept secure.
- Employers are careful when monitoring personal communications such as emails which are clearly personal.
- Employers only undertake covert monitoring in the rarest circumstances where it is used for the prevention or detection of crime.

Appendix 6 – Relevant Legislation

Telecommunications (Lawful Business Practise) (Interception of communications) Regulations 2000
This Act empowered the Secretary of State to make regulations, which allow businesses to intercept communications in the course of lawful business practice and in specific circumstances without the express consent of either the sender or the recipient. Under the Regulations, businesses are required to make all reasonable efforts to inform users of their own systems that such interceptions might take place.

Contract law
It is just as possible to make a legally binding contract via email as it is by letter or orally. Workers need to be aware of the danger of inadvertently making contracts on behalf of their employer or varying the terms of any existing contract.

Copyright law
The Copyright, Designs and Patents Act 1988 (as amended) gives the same protection to digital and electronic publications as it does to printed books and other forms of publication. Many websites carry warnings that the information given is copyright and should not be downloaded without agreement from the copyright holder. Similarly, copyright exists over software, which should not be downloaded without license.

Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988
These Acts are concerned with material that might be criminal, cause harm to young persons or be otherwise unlawful. In the workplace the downloading of certain images from the Internet might subject a worker to charges of criminal behaviour.

Computer Misuse Act 1990
This Act is concerned with the problems of Unauthorised Access into computer systems or ‘Hacking.’ The law covers:

- Unauthorised access to computer material
- Unauthorised access with intent to commit or facilitate a crime.
- Unauthorised modification of computer material
- Making, supplying, or obtaining anything that can be used in computer misuse offences.

Appendix 7 - Lawful Business Practice Regulations (LBP)

The LBP Regulations authorise employers to monitor or record communications **without** consent for a number of purposes, including the following:

- To establish the existence of facts relevant to the business.
- To ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business.
- To ascertain or demonstrate standards which are, or ought to be, achieved by persons using the system.
- To prevent or detect crime.
- To investigate or detect the unauthorised use of telecommunication systems.

The Regulations cover all types of communications including those that are Internet based, by fax and by email.

Appendix 8 – Governors e-Safety Checklist

It is the responsibility of the e-safety Governor and e-Safety Coordinator to ensure that this document is completed and then reviewed once a year at the annual meeting between the two personnel. The results are to be reported to the governing body annually or at the next meeting following a major incident.

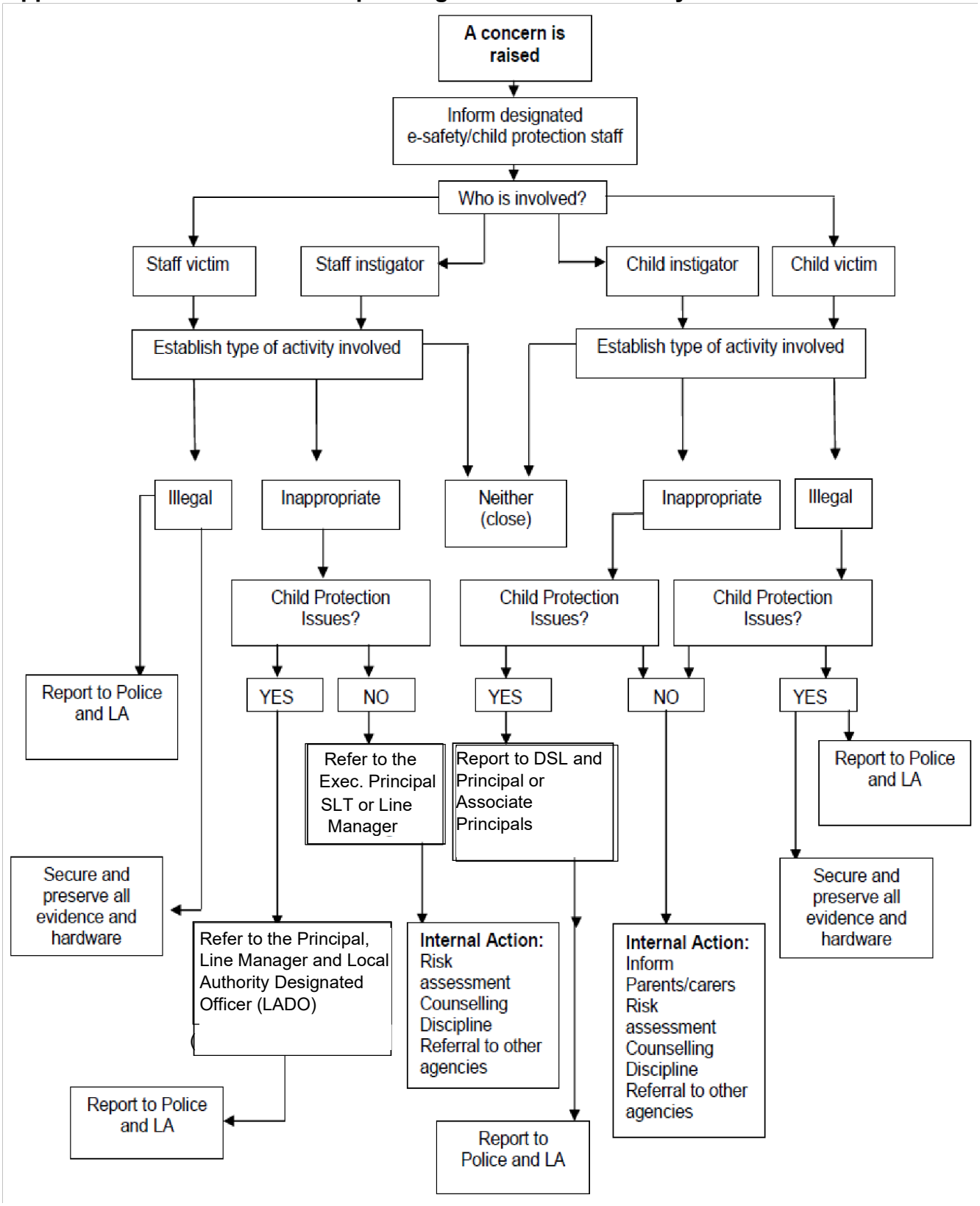
Status	R	A	G	Action/Comments
Appropriate e-Safety policy agreed by governors and in place.				
Appropriate Acceptable Use Policies are in place for all users – signed and stored centrally.				
All staff (teaching and non-teaching) and any volunteers or supply staff are familiar with the current e-Safety policy and the Acceptable Use Policy.				
Staff have received appropriate training for e-Safety, misuse of ICT and inappropriate internet conduct.				
e-Safety, misuse of ICT and inappropriate internet conduct forms part of the induction process for new staff.				
All parents/carers have received a copy of the school's Acceptable Use Policy.				
Appropriate procedures are in place to deal with any e-Safety, misuse of ICT and inappropriate internet conduct incidents that should occur.				
All staff (teaching and non-teaching) and any volunteers or supply staff are informed of how to raise a concern and can gain access to the 'A concern is raised' flow diagram.				
A central record of e-Safety incidents is being recorded – this has been viewed showing the most recent incidents.				
Appropriate filtering is applied to internet content available through the school network.				
Appropriate Monitoring is applied to all school owned devices.				

Online safety, Filtering and Monitoring Audit has been completed.				

E-Safety Governor Signature: _____ Date: _____

E-Safety Coordinator Signature: _____ Date: _____

Appendix 9 – Flowchart for Responding to a Serious e-Safety Incident



(Based on Staffordshire LA Safeguarding Board)

Appendix 10 – Staff ICT Acceptable Use Policy No 44a

Computing Facilities

The school's network of computer systems and devices is owned by the school and is made available to staff to support their professional work. This ICT Acceptable Use Policy has been written to protect all users – students, staff, and the school community. You are responsible for professional behaviour when using the systems, all its resources and the Internet. You are expected to be an active participant in e-Safety education, taking personal responsibility for your own and your students' awareness of the opportunities and risks posed by new technologies.

This policy applies to using school resources both on-site and off-site. You agree and accept that any device loaned to you by the school is provided solely to support your professional responsibilities and that you will notify the school of "any significant personal use" as defined by HM Revenue and Customs, and seek permission for such use from either Associate Principal.

Staff should refer to the full e-Safety Policy (No44) or e-Safety Coordinator for further clarification or details. It is the responsibility of employees to read the latest version of the policy because technology and the law change regularly.

Staff can access the school's internal systems from outside school by using the school provided devices (Laptops / Cloud books / Tablets). These devices will work the same outside of the school as if on site with the only requirement being an internet connection.
If not using a school owned device, then email and file access can be access via the website.

Logging on and Security

- You are responsible for the protection of your own network logon accounts and should not divulge passwords to anyone else.
- Do not let anyone else use your account while you are logged in. Your account is for your use only and should not be accessed by any other pupil, staff, or visitor. Any misuse will be logged against your account, and you will be held responsible for it.
- Always be wary about revealing your home address, telephone number, or school name on the Internet. Personal details of any adult working at the school or student at the school should not be given. (see e-Safety Policy)
- Other computer users should be respected and should not be harassed, harmed, offended, or insulted. (See e-Safety policy)
- Always log off when leaving a workstation, even for a short time.
- To protect yourself and the systems, you should respect the security settings on the computers; attempting to bypass or alter the settings may put you or your work at risk. (See e-Safety policy)

- Any attempts to access, corrupt or destroy others user data, or compromise the privacy of others in anyway, using any technology is unacceptable.
- Computer storage areas are accessible by ICT Services IT Helpdesk staff who may review your files, communications, and computer usage to ensure that you are using the system responsibly. (See e-Safety policy)

Use of the Network and Computer Facilities

All users must take responsibility for their own use of new technologies, making sure they use the technology safely, responsibly and legally.

Whilst using any of the schools IT facilities and equipment staff should observe the following conditions:

Using IT Suites:

- **On arrival and before leaving** the IT suite staff should check the condition of the room. This involves making sure:
    - All computer systems are functional.
    - The printers are functional and have sufficient paper, report to ICT Services if there are any issues or more paper is required.
    - The chairs are in full working order with no damage.
    - The room is tidy with no loose paper or lost property around
    - Before leaving ensure that all computers are logged off

- Any problems with broken/damaged equipment should be reported to ICT Services Helpdesk immediately.
- Lost property should be handed to Reception or returned to the owner if possible.
- During the lesson staff should actively enforce the IT Acceptable Use Policy (copies are available for view in the Staff Handbook and on the staff resources area on the T drive.) Any serious breach of policy should be reported to the ICT Services Helpdesk
- Staff should always ensure correct and appropriate use of equipment such as not placing bags on desks or swinging/spinning on chairs. There should be no food or drink consumed in ant IT room. Any serious problems should be dealt with by the teacher using the school behaviour, rewards, and sanctions measures.
- In the event of damage to equipment or computer malfunction the IT Services Helpdesk should be notified by e-mail immediately.

Monitoring

When in lessons or using the ICT facilities in school, Colchester County High School for Girls monitors in the following ways:

Monitoring Strategy	Colchester County High School For Girls Procedures
Physical Monitoring	Walking around in lessons or using the relevant software for the teacher in charge to monitor what is on each screen.
Internet and web access	Monitored by pastoral team from alerts generated by the web filter. This is reviewed annually.
Active/Pro-active technology monitoring services	Monitored by pastoral team from monitoring alerts. This is reviewed annually.
Using Classroom Management Software	Using Classwize to monitor student screen live within your class

Using IT Equipment

- Staff should ensure that they know how to use the equipment, and this is clearly explained to and understood by the students using the equipment.
- Staff should actively enforce the IT acceptable use policy and make sure that the equipment and work produced using the equipment matches the student guidelines.
- Students may use equipment when not in direct supervision, but it must be returned at the end of the lesson/session and checked by the member of staff who issued the equipment. It is not acceptable to allow students to keep equipment during lunch or break time.
- If equipment is required for use during break, lunch, or afterschool it should be booked and issued to the students by the member of staff who booked it and subsequently returned to this member of staff before the end of the break/lunchtime or after school session.
- Under no circumstances should students be allowed to take equipment home or off the school premises. If it is necessary for staff to take equipment off the school premises, the IT Manager must agree this.
- In the event of accidental damage or equipment malfunction IT Services Helpdesk must be notified immediately by email

General:
Any misuse of equipment or failure to adhere to IT suite common expectations by students should be recorded on SIMS Behaviour Management

Whilst on duty and passing IT facilities available for student use during break and lunch time staff should actively enforce the IT acceptable use policy and IT suite common expectations.

Filtering and Monitoring
Filtering
Online filtering involves using software or hardware tools to control and restrict access to harmful or inappropriate websites and content categories. This can include URL, keyword, or category-based filtering to help shield children from harmful material such as adult content, violence, drugs, Extremism* and hate speech.

Our filtering system manages the following content (and web search):

Discrimination	content that promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010
Drugs / Substance abuse	Content that displays or promotes the illegal use of drugs or substances
Extremism*	Extremism is the promotion or advancement of an ideology based on violence, hatred or intolerance that aims to: 1. negate or destroy the fundamental rights and freedoms of others; or 2. undermine, overturn or replace the UK's system of liberal parliamentary democracy and democratic rights; or 3. intentionally create a permissive environment for others to achieve the results in (1) or (2). (*Gov.UK definition of extremism 2024)
Gambling	Content that enables gambling
Malware / Hacking	Content that promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
Pornography	Content that displays sexual acts or explicit images
Piracy and copyright theft	Content that includes illegal provision of copyrighted material
Self-Harm	Content that promotes or displays deliberate self-harm (including suicide and eating disorders)
Violence	Content that displays or promotes

Online monitoring is about observing and tracking our school community's digital activities, including web browsing, social media interactions and chat conversations.

It aims to identify potential risks, rule violations, and raise alerts that can be acted on. (see P32 for the monitoring table)

It is unacceptable to knowingly:

- Install any unauthorised software. Always get permission from the ICT Services Department before installing, attempting to install or store programs of any type on the computers.
- Damage, disable, or otherwise harm the operation of computers, or intentionally waste resources. This puts yours and others work at risk.
- Introduce a malicious code or virus. If using removable media such as USB memory sticks do not open any files that you suspect may have been infected with a virus or malicious program. The network anti-virus programme should notify you before infected files are opened.
- Try and gain access to an unauthorised area or system.
- Use any form of hacking or cracking software / system.
- Access, download, create, store, or transmit material which is indecent or obscene, or material which could cause annoyance, offence, anxiety or distress to other network users, or material which infringes copyright, or material which is unlawful.
- Use any applications or services to bring the school or its members into disrepute.

The network and computers are provided for professional and educational purposes. You may use the computers for private use in your own time providing that use does not prevent others from using resources for work purposes. (see e-Safety Policy for restrictions)

You have a duty to report failings in technical safeguards which may become apparent when using systems and services. This could include any issues with Filtering or Monitoring

You should protect the computers from spillages by eating or drinking well away from the ICT equipment.

Use of the Internet

Filtering software is used on the school network to prevent access to inappropriate internet sites, and to protect the computer systems. Staff should be aware that the school logs all Internet use.

Access to the Internet is provided for school activities. You may access the Internet for reasonable appropriate private use in your own time providing that use does not prevent others from using resources for work purposes. (See e-Safety policy for restrictions)

Connection to the school wireless network is permitted only for professional/educational purposes only. Connection with personal devices such as

tablets or smartphones permitted only at the discretion of the e-Safety Coordinator, Senior Leadership Team, and ICT Services Department.
Only access appropriate material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene, abusive, or likely to cause anxiety or distress is not permitted. (See e-Safety Policy for definitions)

You should respect the work and ownership rights of people outside the school, as well as other staff or students. This includes abiding by copyright laws. (See e-Safety Policy Appendix 6 for details.)

Use of Email

All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network. Automated software scans all email and removes anything which could affect the security of the computer systems or contain unsuitable or offensive content.

Only the school email account should be used for emails which are sent on school business. You should not use a personal email account for school business. Remember that any emails sent using a school email account are sent on behalf of the school in the same way as official letters. Emails should be professional in language and tone and should not compromise the reputation of the school.

Your school email account should not be used routinely to communicate with family and close friends. Personal email accounts should be used for personal communication and to sign up for mailing lists or online communities that are not school related.

Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, or which is bullying in nature, you should always report such messages to a member of ICT support staff and your line manager.

Emails should not be used during lessons unless it is deemed an emergency. Emails should not be used to communicate with colleagues on aspects that could be deemed of a personal or casual nature.

The sending of an email or text containing content likely to be unsuitable for students or schools is forbidden.

You should only communicate with student via email using your school email address, never use your personal email address to communicate with students. You must not use any other forms of communication that have not been approved by the organization to communicate with students.
You should regularly delete unwanted sent and received e-mails.

Social Media

The use of social media can enhance teaching and learning but is also used widely for social interaction. Teachers should exercise extreme caution when using social media sites such as Facebook and ensure maximum privacy settings. (See e-Safety Policy for further guidance and clarification)

Under no circumstances should a teacher use a personal social media account in the classroom or to facilitate their lessons. It is unacceptable for a member of staff to accept a friend request from an existing student on a personal social media account. See 44c Social Media Policy for further guidance.

Use of Online/Distanced Learning programmes – Teams

When using an online learning platform like Microsoft Teams, staff at Colchester County High School for Girls should ensure that:

- Every Team should have two staff members to safeguard everyone in the Team, the additional person should ideally be a Head of Department or Year Leader
- Staff should ensure that students participating in a live stream has permission from their parents to be there. No permission - No live stream
- Staff and students should establish and follow clear ground rules of that Team (e.g. no speaking over each other, offering rude or silly comments, using it as a private messaging service, sharing personal details). This is likened to a teacher creating the correct climate for learning in their classroom. If live streaming, these rules need to be reiterated every session.
- Students should not record, re-produce or re-distribute materials from the live stream, including taking screen shots. They will be removed from the Team immediately if found doing so and reported to the e-Safety Coordinator.
- All members of the Team participate in live streaming in neutral area, (i.e., not in a bedroom or bathroom). Microsoft Teams has the capability to blur or neutralise a background should the user wish.
- Members of the Team should not disclose personal information to anyone in the stream, such as their location, date of birth or phone number to anyone on the livestream, these should always be kept private. School-allocated email addresses are the only email addresses to be used. Usernames and passwords must never be shared.
- Team members do not have to be visible –audio participation or via live chat only are also acceptable.

- All members of the Team are dressed appropriately (i.e. follows the schools normal non-uniform day dress code)
- Teams should not be used on a one-to-one basis between staff and students. Remote learning on a one-to-one basis is not appropriate.

Personal Laptops / Computers / Devices

Personal laptops / computers / hand-held devices are only allowed to be used in school with permission of the Associate Principals and the IT Manager. Connection to the school network however must be agreed with the Senior Leadership Team, Associate Principals, and ICT Services.

Disciplinary Procedures

If you breach these provisions, access to the network may be denied and you may be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff Code of Conduct and Disciplinary Procedures. Where appropriate, police may be involved, or other legal action taken. (See e-Safety Policy for details).

ICT Services Helpdesk

Any problems or faulty equipment should be reported to the ICT Services IT Helpdesk immediately. You should not attempt to repair equipment yourself.

Mobile Device Encryption

To comply with the Data Protection Act 2018 and GDPR, all school owned devices will be encrypted enabling us to ensure that all data will be kept secure if the device is lost or stolen.
ICT Services will manage encryption. No user other than a person in ICT Services may decrypt the drive on a temporary or permanent basis. Failing to adhere to this will make you liable for any data access breaches which could incur fines.

Remote Data Wipe

Colchester County High School for Girls staff who have access to school email through their mobile phones must accept that ICT Services will have the right to remote wipe the device to prevent any data access breaches if the device is lost or stolen. Failure to notify ICT Services in the event of a device being lost or stolen will render you personally liable for any fines incurred.

Privacy and Personal Protection

- Colchester County High School for Girls staff must always respect the privacy of other students and members of staff; this includes not taking photographs or video or sound recordings.
- Staff should not forward messages (private or otherwise) without permission from the original sender.

- Staff should not supply personal information about themselves or others, on any type of websites or within email.
- When using social media staff must keep all information about school private; especially naming the school which you work at.
- Staff must not upload any pictures or videos taken in school or that show school uniform to any social media sites including Facebook, YouTube, Instagram, WhatsApp, or Snapchat
- Staff understand that all corporate owned devices are filtered and monitored to comply with safeguarding requirements.

ICT Services

Any problems or faulty equipment should be reported to the ICT Services IT Helpdesk immediately. Students or Staff should not attempt to repair equipment themselves.

Please read this document carefully. Only once it has been signed and returned will access to the school computer network be permitted.

I have read and understand the above and agree to uphold the standards outlined within these guidelines and the e-Safety Policy.

Staff Name: _____ Signature: _____Date: _____

Policy links: AT2 Safeguarding & Child Protection Policy A4
Behaviour, Sanctions & Rewards Policy
A5 Anti-bullying Policy
44c Social Media Policy

Reviewed May 2025

Appendix 11 – Student ICT Acceptable Use Policy No. 44b

Computing Facilities

Students are encouraged to make use of the school computing facilities for educational purposes. All students are expected to be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.

Due to high demand for computer facilities at lunchtimes, use of computers at this time must be restricted to schoolwork only. **Students must not be in ICT rooms after school unless supervised by a member of staff.**

Students can access the school's email and online documents by visiting the school website.

Logging On and Security

- You are responsible for the protection of your own network logon accounts and should not divulge passwords to anyone else.
- Do not let anyone else use your account while you are logged in. Your account is for your use only and should not be accessed by any other student, staff, or visitor. Any misuse will be logged against your account, and you will be held responsible for it.
- Other computer users should be respected and should not be harassed, harmed, offended, or insulted.
- You must not log on as someone else, nor use a computer which has been logged on by someone else.
- You should also log off when leaving a workstation, even for a short time.
- To protect yourself and the systems, you should respect the security settings on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Any attempts to access, corrupt or destroy others user data, or compromise the privacy of others in anyway, using any technology is unacceptable.
- Computer storage areas are accessible by ICT staff who may review your files, communications, and computer usage to ensure that you are using the system responsibly.
- You must only use your account on your own devices when using any school provided network access when authorised to do so.

(See e-Safety Coordinator or e-Safety Policy if further clarification is required)

Use of the Network and Computer Facilities

All users must take responsibility for their own use of new technologies, including BYOD devices, making sure they use the technology safely, responsibly and legally. It is not acceptable to knowingly:

- Access, download, create, store, or transmit material which is indecent or obscene, or material which could cause annoyance, offence, distress or

anxiety to any other student or member of the school community, or is bullying or harassing in nature, or material which infringes copyright, or material which is unlawful. This will result in action being taken, according to the School Behaviour Policy.
- Download or install programs to a school owned computer or a BYOD.
- Introduce a virus, or malicious code.
- Bypass network and systems security, breach technical safeguards or conceal network identities.
- Access another student's account.
- Gain access to an unauthorized area or system.
- Use any form of hacking or cracking software / system.
- Use any applications or services to bring the school or its members into disrepute.
- Engage in activities which damage resources, waste teaching or technical support time or use the network resources in such a way to diminish the service for other network users.

(See e-Safety Coordinator or e-Safety Policy if further clarification is required)

Students have a responsibility to report any known misuses of technology including the unacceptable behaviour of others.

Students have a duty to report failings in technical safeguards which may become apparent when using systems and services.

Students must not eat or drink in a designated computer room or near any computer equipment, including a BYOD.

Use of the Internet

Filtering software is used on the Colchester County High School for Girls network to prevent access to inappropriate internet sites, and to protect the computer systems. Students should be aware that the school logs all Internet use.

- The use of public chat rooms is not allowed.
- The use of social networking and video websites is not allowed unless used for educational purposes and approved by the class teacher and/or e-Safety Coordinator
- Students should not copy (plagiarise) and use material from the Internet to gain unfair advantage in their studies, for example in coursework. Such actions may lead to disqualification by examination boards.
- Students should ensure that they are not breaking copyright restrictions when copying and using material from the internet.
- Students must not reveal their own or another student’s personal information such as name, address, telephone number, email address or school name over the internet.

(See e-Safety Policy if further clarification is required)

Online filtering involves using software or hardware tools to control and restrict access to harmful or inappropriate websites and content categories. This can include URL, keyword, or category-based filtering to help shield children from harmful material such as adult content, violence, drugs, Extremism* and hate speech.
Our filtering system manages the following content (and web search):

Discrimination	content that promotes the unjust or prejudicial treatment of people with protected characteristics of the Equality Act 2010
Drugs / Substance abuse	Content that displays or promotes the illegal use of drugs or substances
Extremism*	Extremism is the promotion or advancement of an ideology based on violence, hatred or intolerance that aims to: 1. negate or destroy the fundamental rights and freedoms of others; or 2. undermine, overturn or replace the UK's system of liberal parliamentary democracy and democratic rights; or 3. intentionally create a permissive environment for others to achieve the results in (1) or (2). (*Gov.UK definition of extremism 2024)
Gambling	Content that enables gambling
Malware / Hacking	Content that promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
Pornography	Content that displays sexual acts or explicit images
Piracy and copyright theft	Content that includes illegal provision of copyrighted material
Self-Harm	Content that promotes or displays deliberate self-harm (including suicide and eating disorders)
Violence	Content that displays or promotes

Online monitoring is about observing and tracking our school community's digital activities, including web browsing, social media interactions and chat conversations. It aims to identify potential risks, rule violations, and raise alerts that can be acted on.

Use of Email

All users should understand that network activity and online communications are monitored, including any personal and private communications made via the school network.

- Student email accounts are primarily for communication between students and teachers in relation to schoolwork.
- Students are not allowed to use email during lessons without the teacher's permission.
- If a student receives an e-mail from an unknown person, or which is offensive or upsetting, the relevant teacher or a member of the ICT technical staff should be contacted. Do not delete the email in question until the matter has been investigated.
- The sending / forwarding of chain e-mails are not allowed.
- The sending of a large number of multiple e-mails is acceptable only for good reason. Before doing so, the student must obtain permission from the e-learning coordinator or ICT Services Department.
- Students must not open attachments from senders they do not recognise, or that look suspicious.
- Students should periodically delete unwanted sent and received e-mails.
- Students may use the school email accounts for education use only and not to sign up for any personal services using this address.
- Students should not send emails that cc more than two people. Sending emails to large groups of students or responding to whole year group emails by replying to the whole year group is not permitted.

(See e-Safety Coordinator or e-Safety Policy if further clarification is required)

Use of Online/Distanced Learning programmes – Teams

When using an online learning platform such as Microsoft Teams, students at Colchester County High School for Girls should ensure that:

- Every Team should have two members of staff.
- Students should ensure that they have permission from their parents to participate in live streaming of lessons at Colchester County High School for Girls. Their parents should have signed the Live streaming consent declaration. No permission - No live stream
- Students should follow the clear ground rules any Team (e.g. no speaking over each other, offering rude or silly comments, using it as a private messaging service, sharing personal details).
- Students should not record, re-produce or re-distribute materials from the live stream, including taking screen shots. They will be removed from the Team immediately if found doing so and sanctioned using the school's Behaviour, Rewards and Sanctions Policy
- All members of the Team who participate in live streaming do so in a neutral area, (i.e., not in a bedroom or bathroom). Microsoft Teams has the capability to blur or neutralise a background should the user wish.

- Members of the Team should not disclose personal information to anyone in the stream, such as their location, date of birth or phone number to anyone on the livestream, these should always be kept private. School-allocated email addresses are the only email addresses to be used. Usernames and passwords should never be shared.
- Team members do not have to be visible –audio participation only is also acceptable.
- All members of the Team are dressed appropriately (i.e. follows the schools normal non-uniform day dress code)
- Teams should not be used on a one-to-one basis between staff and students. Remote learning on a one-to-one basis is not appropriate.
- If students are concerned or suspicious about any activity on Teams, they should report it to their Year Leader.

Personal Laptops / Computers / Devices

Non-BYOD devices for example personal laptops / computers and hand-held devices are only allowed in school with written permission from the Year Leader who will specify the times when they can be used. Connection to the school network is only granted with permission from the ICT Services Department following discussion with the Senior Leadership Team. Filtering software will be used to prevent access to inappropriate internet sites, and to protect the computer systems.

Use of Other Technology

Technology such as media rich phones, Personal Digital Assistants (PDA), tablets (including iPads), e-readers, memory cards, USB Storage devices and anything else that can be used to store, transmit or manipulate data should be used responsibly, and in accordance with the e-Safety Policy and used only during the times specified to students. To be able to write any data to any USB media, the media must first be encrypted using Bitlocker. Mobile phones should be always turned off during the school day, including at break and lunch times, in accordance with School Behaviour, Rewards and Sanctions Policy. Year 12 and 13 students are allowed to use their mobile phone in the Sixth Form Common Room area only.

Privacy and Personal Protection

- Students must always respect the privacy of other students and members of staff; this includes not taking photographs, video, or sound recordings.
- Students should not forward private messages without permission from the original sender.
- Students should not supply personal information about themselves or others, on any type of websites or within email.
- People you contact on the internet are not always who they seem, therefore, students must not attempt to arrange meetings with anyone met via a website or email.
- When using social media students must keep all information about school private; especially naming which school is attended.

- Students must not upload any pictures or videos taken in school or that show school uniform to any social media sites including Facebook, YouTube, Instagram, WhatsApp or Snapchat or any other social networking site that is in existence.
- Students should realise that the school has a right to access personal folders on the Network and/or confiscate personal technologies such as mobile phones. Privacy will be respected unless unacceptable use is suspected.
- Students understand that all corporate owned devices are filtered and monitored to comply with safeguarding requirements. This also includes BYOD devices.

Disciplinary Procedures

Violation of this ICT Acceptable Use Policy may result in a temporary or permanent ban on network use. Additional disciplinary action may be taken in line with the School Behaviour, Sanctions and Rewards Policy. Where appropriate, police may be involved, or other legal action taken. (See e-Safety Policy for further details)

ICT Services

Any problems or faulty equipment should be reported to a teacher or ICT technician immediately. Students should not attempt to repair equipment themselves.

Please read this document carefully. Only once it has been signed and returned will access to the school computer network be permitted.

I have read and understand the above and agree to uphold the standards outlined within these guidelines and the e-Safety Policy.

Student Name: _____ Signature: _____

Date: _____

Appendix 12 – Social Media Policy No. 44c

Introduction and Context

This policy governs the publication of and commentary on social media by associates of Colchester County High School for Girls. This extends to employees, governors, students, parents, and any other personnel associated with the school. For the purposes of this policy, social media means any facility for online publication and commentary, including without limitation, blogs (including blogs on platforms like Instagram), wiki's, social networking sites such as TikTok, Facebook, LinkedIn, X (formally known as Twitter), Flickr, and YouTube. This policy is in addition to and complements any existing or future policies regarding the use of technology, computers, e-mail, and the internet. These are outlined below in the policy links.

Colchester County High School for Girls associates are free to publish or comment via social media in accordance with this policy. Colchester County High School for Girls associates are subject to this policy to the extent they identify themselves as having association with Colchester County High School for Girls.

Social Media refers to a multitude of media facilities that allow users to interact socially. They offer many different types of computer-mediated tools that allow people or companies to create, share, or exchange information, career interests, ideas, and pictures/videos in virtual communities and networks.

Social Media has developed into a powerful tool for education, but it is also a platform that is open to potential abuse. The purpose for this policy is to clarify expectations of associates of Colchester County High School for Girls and to offer help and advice on the use of social media both professionally and personally.

Publication and commentary on social media carry similar obligations to any other kind of publication or commentary.

All uses of social media must follow the same ethical standards that Colchester County High School for Girls associates must otherwise follow.

Policy links:

- 44 e-Safety Policy
- A3 Safeguarding & Child Protection Policy
- A4 Behaviour, Sanctions & Rewards Policy
- A5 Anti-bullying Policy
- 26 Code of Conduct
- 44a ICT AUP Policy - Student
- 45 ICT AUP Policy - Staff
- ICT Communications Procedures and Guidance for Staff (in Staff Handbook)
- 44d Generative Artificial Intelligence Policy

Please Note: This e-Safety Policy has been written by Colchester County High

School for Girls e-Safety Coordinator. It has been agreed by Colchester County High School for Girls Governing Body, Senior Leadership Team, ICT Services, and the e-Safety Coordinator.

Professional Use of Social Media as an Educational Tool

Colchester County High School for Girls actively encourages the use of appropriate Social Media platforms for educational benefit inside and outside the classroom environment. Although departments are actively encouraged to have a Social Media presence these expectations must be met:

- When making the decision to create a departmental account/page/group/channel or any other Social Media facility that associates with Colchester County High School for Girls or a department within, notification must be provided to the Senior Leadership Team and the e-Safety Coordinator.
- Following notification, a request for approval may be issued. In such cases any activity on the social media platform in question must be withheld until approval is granted.
- The terms of service must be followed on all platforms of social media.
- Social Media presence from a particular individual or a department must clearly identify its association with Colchester County High School for Girls. For example, a Facebook page created by the PE department might be called: "Colchester County High School for Girls PE Department" or the Twitter handle used by computing teacher "@StaffNameCCHSGIT" but the account named "*Colchester County High School for Girls Computing Department."*
- It is appropriate to allow multiple personnel who belong to a department to make posts however, posts must only be made from the departmental account or other professional only account and in no way from an employee's personal or private account.
- It is an expectation that employees (this extends to those in temporary employment or employment by association such as trainee teachers) will do all that they can to disassociate personal or private social media accounts with those created for educational purposes. This will only increase the risk of potential invasion of privacy. For example, a member of staff should not post from their personal Facebook account onto the Facebook page that has been created for the department in which they work. If they wish to make posts on the page they should seek permission to do so from the Head of Department and be granted permission to do so as a page administrator or create a professional account that clearly identifies them and associates them with the school and department and that is used solely for professional/educational use then use this account to make posts on the departmental page. Employees should not like or follow the professional pages/accounts of the school, employees, or the departments thereof from their personal accounts.
- It is acceptable for all other associates (not employees) including, students, governors, and parents to create social media interactions (such as likes, comments, favourites, retweets etc.) from their own personal pages provided

these interactions are appropriate. Appropriate social media interactions outlined below.

- For this explanation, all social media interactions will be referred to as posts. All associates of Colchester County High School for Girls must only make posts on any social media platform pages/accounts of the school, employees, or the departments thereof that are appropriate. This means that no words/images/videos/links or any other type of digital media that are deliberately offensive, hateful, incite violence, racism, extremist views, dangerous and unlawful activities, sexual reference or nudity, any activity that does not safeguard the students and employees of Colchester County High School for Girls, that expose private personal details of others, that degrade the school or any other organisation.
- Departmental or individual professional pages should create a link (such as a follow or friend) with the school official account, when possible, on the same platform. This serves as authentication of the account and as moderation/supervision of content posted. It is expected that the school official account with share/retweet/favourite/repost/like/comment on as significant posts made from the department account.
- Posts made should serve the purpose of improving the communication and promoting the school and individual department. Posts should have significance to the activities in the department or subject area and/or be educationally beneficial.
- If any associate is in doubt about making a particular post regarding its content or intentions, then caution should be exercised. Seek advice from the Head of Department or from the e-Safety coordinator before posting or choose another more appropriate method of communication for said information.

  Advice and tutorials on how to set up departmental social media Accounts can be sought from the e-Safety Coordinator and ICT Services Department.

Personal Use of Social Media Advice for Employees

- Employees of Colchester County High School for Girls should exercise caution when online and use social media responsibly. General advice for staying safe online and responsible use of social media can be found in appendix 1.
- The terms of service must be followed on all platforms of social media.
- Personal use of Social Media accounts by employees is acceptable but not essential for those using social media professionally. A personal Social Media presence should be as separate from their professional accounts as possible much in the same way that you separate your real-world personal life from your professional life.
- An employee's personal Social Media interactions should uphold the high standard of professional, social, moral, spiritual, cultural, and ethical behaviour that is expected of secondary school employees.

- Posts should always be appropriate as outlined in the previous section of this policy.
- An employee should take all actions to disassociate their personal Social Media accounts with those of the school or school departments.

It is acceptable for an employee to identify them as an employee of Colchester County High School for Girls where applicable on Social Media platforms but all other references to school activity should be minimised.

A member of staff's personal Social Media accounts and subsequent posts should use the highest level of privacy settings that only allow views/interactions from those that have been accepted as a friend/follower.

- Privacy settings should be regularly reviewed and adjusted so as maintain the highest levels of privacy. In addition, a regular review of friend and follow lists should take place.
- It is not appropriate for an employee to accept a friend/follow request from students on roll in the school. It is advisable that staff exercise professional judgement and caution in accepting requests from students who are no longer on roll but may still have links with other students in school.
- Employees should exercise professional judgement in accepting requests from close family members of existing students.
- Employees should not make posts/interactions that have direct reference to school activities/policy from personal accounts. Any such interaction should be carried out solely from professional accounts. For example, it would be inappropriate for an employee to post comments and images about activities taken place in a particular lesson from their personal Social Media account, but it would be completely appropriate to do so from their professional/departmental account.
- It would be considered inappropriate and unprofessional for a member of staff to make any posts that portray negativity or degradation towards the school, school activities or towards other employees or associates of Colchester County High School.

Advice for other associates (including students)

- Associates of Colchester County High School for Girls should exercise caution when online and use social media responsibly. General advice for staying safe online and responsible use of social media can be found in appendix 1.
- The terms of service must be followed on all platforms of social media.
- Students and their parents are strongly advised to adhere to age restrictions in place on certain social media platforms.
- It is acceptable for associates of Colchester County High School for Girls to follow/friend/subscribe to pages/accounts/groups created by the school, departments, or as professional accounts by employees.
- It is unacceptable for students to request/friend/follow/subscribe the personal accounts of employees of Colchester County High School for Girls. Other

associates should exercise caution in sending a request to avoid compromising the employee's professional integrity.

Posts and all interactions to school official social media or employee's professional accounts must be appropriate as outlined in the previous section of this policy.

- Staff, students, and the wider community are not permitted to create posts including images/video footage/any other media that have been captured on the school premises or that show a student or group of students wearing school uniform. Such posts are only permitted from the school official Social Media accounts or staff/ department professional accounts.

Using Social Media During School Hours

- The only acceptable use of social media during school hours and/or using the school facilities is for the purposes of education. It is unacceptable for staff, students, or any associates of Colchester County High School for Girls to access personal Social Media accounts for any non-school related activities either in lesson time or any other time during the school day.
- The above condition applies in-particular to accessing personal Social Media accounts through mobile devices connected either through Colchester County High School For Girls Wi-Fi or personal mobile data provider.

Social Media in Lessons

- It is appropriate to use social media during lessons provided the platform is suitable for the context of the lesson. Teaching staff however should note that in planning to use social media in a lesson that some platforms will not be accessible through the school web filtering solution.
- It must be accepted by employees that; if a particular platform is blocked by the web filter for students, then it is not suitable for use by students in school, if a particular platform is blocked by the web filter for employees then it is not suitable for use in school at all.
- If a lesson is being delivered and is making use of students being able to access their personal accounts for the purpose of the lesson the teacher should exercise caution to make sure that the activity is being carried out as planned and the Social Media interactions carried out by the students are appropriate for the purpose of the lesson.
- In some cases, it may be appropriate to use school owned mobile devices and the use of an appropriate Social Media software App to facilitate the lesson. This is appropriate but agreement must be made beforehand with ICT services to have the appropriate App pre-installed and connection to Wi-Fi available. Teaching staff must also take particular care to log out of their account on the device they are using and to remind students to do so also. Personal devices must not be used without permission from the Senior Leadership Team.

  At present it is not acceptable to allow students in Years 7 to 9 to use personal mobile devices to connect to Colchester County High School for Girls Wi-Fi. Year 10 and 11 will have limited access during public

examinations for revision purposes only. In addition, it is not appropriate to allow any student to use personal mobile devices to access social media for the purposes of a lesson even using a personal mobile data provider.

- In special circumstances, such as an educational visit where students have been granted permission to carry their own mobile devices, students may use social media from their personal devices so long as the intention is to enhance the learning experience. They are not permitted to create posts including images/video footage/any other media that have been captured to show a student or group of students wearing school uniform. Such posts are only permitted from the school official Social Media accounts or staff/ department professional accounts.

Policy Violations and Responding to Misuse

Policy violations and the response to these will be treated as an e-Safety policy violation and use the same procedures will be followed.

If you have made a mistake and unintentionally caused a policy violation or another problem, then the best policy is to be honest and act quickly. Social Media can be powerful tool both in the promotion and defamation of an individual so a fast and honest response to a mistake is the best procedure to minimise the impact. Discuss the problem immediately with your line manager and report to Senior Leadership Team and/or the e-Safety coordinator.

If the mistake relates to a particular post/social media interaction, then a physical record should be taken such as a screenshot or even just a photograph. Then the post or interaction should be removed/undone as quickly as possible. If unsure on the best course of action, then consult the e-Safety Coordinator or ICT services with the support of your line manager.

Appendix 13 – 44d Generative Artificial Intelligence Policy

When using generative Artificial Intelligence (AI) it is important that our school ensures we can maximise the benefits of AI while minimising any risks or concerns.

This policy sets out the rules all staff, voluntary workers, agency staff, contractors, and other third parties working on behalf of the school **must** follow when using generative AI.

Policy rules

1. You must only use AI applications authorised by our school. Authorised services can be found by contacting ICT Services who hold an accurate list of services available for use.

2. You must select the opt-out option before first use of authorised AI applications if applicable. This will prevent the data you enter into the prompt being used by the Large Language Model (LLM) to train itself. If the opt out selection is unclear or is not available on the authorised AI application, please contact the school Data Protection Lead for further clarification.

3. When using any of the authorised AI applications, you must use your work email address for log-in purposes.

4. Before using an AI application you must have authorisation from the schools Data Protection Lead and ICT Services.

5. When using AI applications you must ensure that confidential, sensitive, or proprietary employee, student, parent/carer or third-party supplier, including personal data or sensitive data, is **not** entered into the application as a prompt in breach of data protection legislation.

6. If your use of AI applications will involve any personally identifiable data you **must** complete a Data Protection Impact Assessment (DPIA) and where necessary an Equalities Comprehensive Impact Assessment (ECIA), both approved by the school prior to any use.

7. You must be aware of, and comply with, any intellectual property rights (IPR) or licencing conditions and include referencing of your sources when using AI tools.

8. You must not input offensive, discriminatory or inappropriate content as a prompt.

9. You must comply with our Information Security and Data Protection Policies when using AI applications or any other technologies.

10. You must carefully review any AI outputs to guard against bias, inappropriate or offensive data.

11. You must not generate content to impersonate, bully, or harass another person, or to generate explicit or offensive content.

Why must I comply with these policy rules?

These policy rules will help us to comply with the law and regulatory guidance when using artificial intelligence. The use of generative artificial intelligence (generative AI) is transforming the way individuals are working. Informed and responsible use of generative AI has the potential to increase efficiency in the workplace, improve decision making and foster innovation. With these benefits come potential risks, including data protection breaches, copyright issues, the protection of confidential information, ethical considerations and compliance with wider legal obligations. AI systems learn based on the information you enter. Just as you would not share work documents on social media sites, do not input such material into generative AI tools.

Large learning models (LLMs) are a type of generative AI that can generate human like text in response to a prompt. They use deep learning techniques and massive data volumes to generate a response. LLMs can produce outputs which may initially appear to be believable but are in fact highly inaccurate or fabricated. This is known as a hallucination. AI needs personal data for training the LLM so it can mimic human behaviour, and lots of it to improve accuracy. Currently there are no reliable techniques for steering the behaviour of LLMs which are very complex to understand. This increases data protection risks as well as the risk of unconscious bias. AI applications must be used ethically and responsibly to avoid harm, reputational damage, unlawful processing and regulatory censure.

It is essential that we complete due diligence checks on any AI application the business are considering using to ensure it meets ethical and legal conditions, reducing risks for the business and individuals. AI platforms can involve collaboration between multiple parties or use third-party tools and services. This increases the risk of unauthorised access or misuse of personal data, especially when data is shared across jurisdictions with different privacy regulations.

Since generative AI models take unstructured prompts from users and generate new, possibly unseen responses, you need to protect personal or sensitive data in-line. Many known prompt-injection attacks have been seen in the wild. The main goal of these attacks is to manipulate the model into sharing unintended information.

You must always comply with our Code of Conduct and our Policies and consider the need to complete an Equalities Comprehensive Impact Assessments (ECIAs).

Every member of staff is responsible for assuring the security of any processing by the school. AI can be misused for malicious purposes, such as automating cyberattacks or creating sophisticated phishing scams. Attackers can leverage AI to launch more targeted and efficient attacks, making it harder for traditional security measures to detect and mitigate them. You must be vigilant and ensure that all technical and organisational controls are complied with to fully protect the data.

Generative AI has the potential to produce inaccurate outputs or hallucinations. There is also a risk that the output is biased, inappropriate or otherwise offensive. This means that critical thought must be applied to all outputs of authorised AI applications; they must always be fact and sense checked before being relied upon for business purposes and reviewed to ensure content is appropriate. These tools can produce credible looking output. They can also offer different responses to the same question if it is posed more than once, and they may derive their answers from sources you would not trust in other contexts. Therefore, be aware of the potential for misinformation from these systems.

How must I comply with these policy rules?

You cannot use AI applications without first seeking and gaining written permission from the school Data Protection Lead. You must select the 'opt out' option, and if one is not available, seek advice from the school Data Protection Lead. You must fully comply with policy and guidance to protect data from cyber threats, reducing risks for individuals and the organisation. You must always use your work assigned email address to enable clarity that AI use has been approved by the business.

To assess the data protection risks of proposed uses of AI applications you must complete a DPIA. Any identified risks must be mitigated to an acceptable level before the DPIA can be approved and the use of AI commenced. Where AI involves the use of personal data you must be able to inform individuals of their data protection rights and how to exercise them. Your privacy notices must be clear if AI activities including the use of personal data. In addition you should provide explanations to data subjects of the process, fairness, outcome and impact to reassure data subjects and enable and inform challenges. The ICO provide guidance on how to ensure you meet data subjects rights when using AI.

You must read and apply the DfE guidance for education sector on the use of generative artificial Intelligence.

Identify and abide by any relevant licensing conditions regarding intellectual property rights in the authorised AI application's terms of use and ensure that third party proprietary data or material is not entered into the application as a prompt without the third party's permission. This includes ensuring, for example, that all or any substantial part of any copyright work owned by a third party is not inputted into the application as a prompt without the third party's consent. Records of checks for copyright, or licencing information, must be evidenced. Whether using the outputs from generative AI either verbatim or with minor alterations, it is important to make clear to those reading that an AI tool has been used. To do this the tools should be cited in a footnote, with its URL and any sources used as inputs.

AI tools, such as a LLM, answer questions by choosing words from a series of options it classifies as plausible. These tools cannot understand context or bias. Always treat with caution the outputs these tools produce and challenge the outputs using your own knowledge and judgement. Outputs must always be fact and sense checked before being relied upon for business purposes and reviewed to ensure content is appropriate. Always apply the high standards of rigour you would to anything you produce, and reference where you have sourced output from in one of these tools.

Always use authorised AI applications ethically and responsibly, taking into account our policies and research governance.

We reserve the right to monitor all content (including but not limited to any prompts, or outputs) on any generative AI application used for school purposes. This will only be carried out to the extent permitted by law, in order for us to comply with a legal obligation or for our legitimate business purposes, including, without limitation, in order to:

a) prevent misuse of the content and protect our confidential information (and the confidential information of our staff, students, parent/carers and suppliers);

b) ensure compliance with our rules, standards of conduct and policies;

c) monitor performance at work;

d) ensure that our workforce does not use our facilities or systems for any unlawful purposes or activities that may damage our school or reputation;

e) comply with legislation for the protection of intellectual property rights and to support proprietary rights in the output.

What if I need to do something against this policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school Data Protection Lead.

If you believe the policy does not meet your business needs, you may raise this with your school Data Protection Lead who, if they agree with your suggestion, may propose a policy change.

Incident Reporting

In the event of any incident involving AI, from technical support to any suspected data breaches, please contact ICT Services.

References

- Data Protection Act 2023/ UK GDPR
- The Intellectual Property Act 2014
- Human Rights Act 1998
- Generative artificial intelligence (AI) in education - GOV.UK (www.gov.uk)
- Guidance to Civil Servants on use of generative AI
- Our work on Artificial Intelligence | ICO
- ICO – Explaining Decisions made with AI
- ePrivacy legislation
- Education legislation
- Marketing legislation

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix 14- General Advice for Online Safety and Responsible Use of Social Media

With all online activity the general rules that we educate our associates to follow and promote are:

- Keep all personal information secret (do not post online anywhere) especially real names (and the names of friends and family), address and postcode, email address and the school you attend.
- Take particular care of the passwords you use for all user accounts – use a secure password (for further guidance see video link below), never ever share these with anyone especially doing so online, do not write passwords down, do not allow other users to access or use any of your accounts.
  https://www.commoncraft.com/video/secure-passwords
- Regularly review privacy settings on your social media accounts, it should only ever be acceptable for people who you have accepted as friends to be able to access your profile and see the posts you make. You must choose settings that do not allow your profile or posts to be available publicly or to users that you have not accepted friend requests from; failure to do so puts you and others at risk.
- Friend/follower requests should only be accepted on the basis that they are family members or existing friends that you know and can trust. It is highly risky to make online friends without knowing who they really are; this puts the user and all their friends at risk.
- Never meet up with anyone with whom you have only had online contact with, you can never really trust someone to really be who they say they are. If you do think you can trust an online friend and want to meet in person, this must be a carefully considered decision discussed with your parents; the only way that is ever acceptable is to meet in a busy place with parents present for supervision.
- Take particular care if receiving emails/messages from people you do not know or messages from existing contacts that look unusual or out of the ordinary in any way. Suspicious messages are often Phishing attempts which could cause the security of your computer system to be compromised by becoming infected with a computer virus or spyware. Do not follow any web links within a message unless you are completely sure what the link is and that it is safe.
- Always be wary when someone tries to contact you online. Try to establish if you do know the person and they are really who they say they are – use a few questions or make some comments that only your friends would genuinely understand and know the answers to. Remember it can be easy for someone to see your online friends or those of your friends,
  pick a name and then create an account in that name and pretend to be that person.
- It is vitally important that you report any suspicious online behaviour or any thing that makes you feel uncomfortable. You can tell your parents or another

adult you trust, a teacher at school, report it directly to CEOP or the local police, or even just share it with a friend who can help. Even if you do not experience something directly or do not feel threatened it is still your duty to report inappropriate online behaviour to the appropriate personnel. Your actions may prevent the suffering of someone else.

We strongly advise parents to discuss the use of these and other platforms that your children might be using.

It is only acceptable for your children to use these social media if you have first given them permission to do so. This should be an informed decision that pays respect to the age restrictions and general terms of use.

Find out what the platform allows users to do and how your children use it. There is joint responsibility between the parent and child to use social media responsibly and parents should be proactive in monitoring their child's online activity much in the same way that you monitor other real-world social interactions. This can be carried out as a bonding exercise between you and your child; you can agree to allow them to use the platform so long as they periodically talk you through their activity and teach you how to also use the platform. If this is done from an early age and frequently enough it can be normalised and be as simple as discussing "what did you learn at school today?" or "who did you spend lunchtime with?"

A simple rule you can observe when deciding to allow your child to use a social media platform is that they can do so if they also help you create your own account, show you how to use it and accept you as a friend. This will allow you to monitor your child's activity without being too intrusive or time consuming.
Depending on the age of your child you may also want to discuss having full access to your child's account or applying the use of parental controls. There should be clear boundaries that both parent and child observe.

Most social media platforms have parental control features or at least a help and advice section aimed at helping parents improve the safety of the platform. A simple internet search of the terms "parental controls…" and the name of the platform will return the results and advice you are looking for.

These websites listed below are particularly useful in helping parents find out more about online safety and key facts about the social media platforms young people are using.
Net Aware - https://www.net-aware.org.uk/networks/

Common sense media - https://www.commonsensemedia.org/

Internet Matters - https://www.internetmatters.org/

Think U Know for Parents/Carers - https://www.thinkuknow.co.uk/parents/

Please read this document carefully. Only once it has been signed and returned will access to the school computer network be permitted.

I have read and understand the above and agree to uphold the standards outlined within these guidelines.

Student Name: _____ Signature: _____

I have read and understood the above and agree to support my child to uphold the standards outlined within these guidelines.

Parent / Carer Name: _____ Signature: _____

Date: _____

Policy links: Alpha Trust Safeguarding & Child Protection Policy A4
Behaviour, Sanctions & Rewards Policy
A5 Anti-bullying Policy
44. E-Safety Policy
44c Social Media Policy

Reviewed May 2025

Appendix 15 – Advice for Staff for Online / Distances Teaching and Learning

There are the occasions where Teaching and Learning needs to be delivered online. This is a guide for staff to deliver lessons online, whilst still maintaining high standards in learning, whilst keeping e-Safety to a premium. Live streaming is a valuable way to connect with the wider community, but staff must be aware of students' online safety.

Planning and setting work:

- All lessons/work should follow the Schemes of Work agreed by the Head of Department and be in line with what would be normally taught in a classroom where possible.
- A note of the work planned should be made in the staff planner as per normal Teaching and Learning expectations.
- Instructions should be explicit, limiting any doubt by the student. Instructions can be built into a presentation or as a separate document.
- All work should be uploaded onto the Colchester County High School for Girls relevant TEAMs page, and a separate school email should be sent to Students alerting them to the upload. Staff should be mindful of the time work is uploaded; this should be completed within the confines of the working day (i.e. up to 18.00) and not late into the evening.
- All communication about work should be via school email in the first instance.
- Staff should be mindful of the length of time tasks may take and plan accordingly. This main mean that something which would normally take one lesson in normal circumstances may take two.
- If online learning occurs for a longer period of time i.e. more than a week, staff should plan for a consolidation lesson at least once fortnightly to embed and consolidate the learning completed at home.
- If staff are setting work which requires an element of on-line research, safeguarding advice should be issued to students.
- All links, clips or AI generated materials should be quality assured before posting in a learning resource.
- Staff must take the usual care when producing learning materials, considering the difficulties individual students may have if a topic is personally difficult for them or may trigger a response which would need one to one support from a member of staff.

Delivering work via Teams:

Staff can deliver their planned work via Teams if they so wish. This is an online platform that allows teachers to either simply upload work to the platform and respond in writing to students during or after the lesson via a specific Team; or pre-record content, to record over PowerPoint presentations, as well as the capacity to 'Live Stream.'

Every organisation that provides Live Streaming activities for students should gain consent from parents or carers for their child to participate. It is also important to gather the necessary information to keep children safe during the activity.

When setting up your Teams, it is the responsibility of the member of staff to ensure the correct security settings are in place, with Staff having clear ownership of the Team, not the students. Staff should be fully aware of the functionality of the system and how to use it before embarking on activities. Staff also have the option to limit the activities students can do, e.g., to limit the chat function, limit the use of emoji type symbols or stickers. Staff should clearly articulate to students the rules of the Team and that they can remove students from a Team should they break any of the 'rules.

The basic rules everyone at Colchester County High School for Girls should follow are:

- Every Team should have two staff members to safeguard everyone in the Team, the additional person should be a Head of Department or Year Leader
- Staff should ensure that students participating in a Live stream has permission from their parents to be there. No permission, no Live stream
- Staff and students should establish and follow clear ground rules of that Team (e.g., no speaking over each other, offering rude or silly comments, using it as a private messaging service, sharing personal details). This is likened to a teacher creating the correct climate for learning in their classroom. If live streaming, these rules need to be reiterated every session.
- Students should not record, re-produce or re-distribute materials from the live stream, including taking screen shots. They will be removed from the Team immediately if found doing so and sanctioned in line with the school's Behaviour, Rewards and Sanctions Policy.
- All members of the Team participate in live streaming in neutral area, (i.e., not in a bedroom or bathroom), or with the background blurred.
- Members of the Team should not disclose personal information to anyone in the stream, such as their location, date of birth or phone number to anyone on the livestream, these should always be kept private. School-allocated email addresses are the only email addresses to be used. Usernames and passwords should never be shared.
- All members of the Team are dressed appropriately (i.e. follows the schools normal non-uniform day dress code)
- Teams should not be used on a one-to-one basis between staff and students. Remote learning on a one-to-one basis is not appropriate.
- Only school registered accounts to be used, never any personal accounts.

Marking work via Teams

Staff should clearly articulate to students which piece of work will be specifically marked and in what way. Staff may choose to do this using the Assignment section of Teams. Any work set in this way should be marked, either online or by other means, and follow the marking guidelines set out in the whole school marking policy. This includes frequency of marking and quality of the formative comments made. There is the ability to set up quick tests and quizzes in Teams. Staff should follow their departmental guidelines when marking these types of activities and make a record of all marks in their mark books.

Appendix 16 – Cyber Security Policy

Introduction

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.
This Cybersecurity Policy outlines Colchester County High School for Girls guidelines and security provisions which are there to protect our systems, services, and data in the event of a cyberattack.

Scope of Policy

This policy applies to all Colchester County High School for Girls staff, contractors, volunteers, and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

Risk Management

Colchester County High School for Girls will include cybersecurity risks on its organisational risk register, regularly reporting on the progress and management of these risks to Governors 3 times a year.

Physical Security

Colchester County High School for Girls will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to, air conditioning, lockable cabinets, and secure server/communications rooms.

Asset Management

To ensure that security controls to protect the data and systems are applied effectively, Colchester County High School for Girls will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing fraud, they must change their password and inform Colchester County High School for Girls ICT Services as soon as possible. Personal accounts should not be used for work purposes. Colchester County High School for Girls will implement multi-factor authentication where it is practicable to do so.
To access any school data, services or devices, the minimum required is for a username and password for authentication. Where possible, multifactor authentication will be enabled when accessing data outside of a corporate owned device.

Any accounts that are no longer in use, whether this is a regular user, guest, or administrator, these will be disabled as soon as they are no longer required.
User accounts are automatically created and disabled from the start and end date displayed the in the organisational management information system. Any staff joining the organisation, or other areas of, that require a user account will have a form completed by HR, requesting the account to be created with the details provided. This is also the same for any leavers if they are not on the organisational management information system.

User accounts created, manually or automatically, will only have the required access relevant to their role. No users are set as local administrators on any devices. Any accounts created for third party services are only assigned the relevant access required for that role / service. Blanket permissions which include access to data or services not required for that role should not be assigned. Any access requests must come from their line manager or an account that has existing access and are in a role who are able to be able to make the request.

Any change in role within the organisation needs to be assessed against the current level of access and if any access needs to be removed or added, a request will then need to be made to the ICT Services department to action the change.
Global administrator or domain administrator accounts should not be routinely used for day-to-day business.

Password for any account must be at least 14-characters long be considered complex. A complex password policy is being enforced. Accounts must also be locked if the incorrect password has been entered for than ten times within a 15-minute window. In the event the account is locked, this will remain locked for 15 minutes before resetting.

At the time of the end of the employee's contract, the data held on the account will be removed. It is the responsibility of the employee and the line manager to ensure that any handover has taken place before the end of contract to ensure a smooth transition of roles. This includes files held within OneDrive, Exchange Mailbox data and any separate teams that may have been created. Teams created automatically will remain.

Devices
To ensure the security of Colchester County High School for Girls issued devices and data, users are required to:

- Lock devices that are left unattended.
- Update devices when prompted.
- Report lost or stolen equipment as soon as possible to Colchester County High School for Girls ICT Services
- Change all account passwords at once when a device is lost or stolen (and report immediately to Colchester County High School for Girls ICT Services)

- Report a suspected threat or security weakness in Colchester County High School for Girls systems to the IT Manager

Devices will be configured with the following security controls as a minimum:

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / malware software
- Automatic security updates for software, operating system, and anti-virus / malware
- Removal of unrequired and unsupported software
- Autorun disabled.
- Minimal administrative accounts
- Filtering and monitoring configured.

To ensure the continuity of device security across the organisation, end users are not permitted to make any changes to the devices in use. Any changes required can be requested to the ICT Services Department for consideration.

Where possible, service accounts are to be used for running system services in lieu of user accounts for services. This is not always possible due to the nature of the service it is running, but where possible, all attempts should be made to ensure system services are running as services accounts.

Data Security

Colchester County High School for Girls will respond appropriately to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data. Colchester County High School for Girls defines confidential data as:

- Personally identifiable information as defined by the ICO.
- Special Category personal data as defined by the ICO.
- Unpublished financial information

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology.

- At least three versions of data
- At least two different types of media
- At least one copy offsite/offline

Access to backups must be limited to technical staff whose role may entail restoring or requiring access to the backups. This must be an identifiable account and have multi factor authentication enabled.

Any backups must be assessed to ensure that the backup has been successful. This could be in the form of a file restore or virtual machine restore. This could be in the form of an automatic or manual testing procedure.

Any data that is encrypted to comply with security and GDPR must have a strong level of cryptographic algorithms, weak cryptographic algorithms are not to be used.

Access to data must be assigned to users based on if they need access to the data. If the role does not require access to the data, then access should not be available. This prevents are unauthorised access to data from users where permission has not been granted. Blanket permissions to access data will not be used.

Sharing Files

Colchester County High School for Girls recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a data breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked.' If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites.
- Wherever possible, keeping Colchester County High School for Girls files on school systems.
- Not sending school files to personal accounts
- Verifying the recipient of data prior to sending
- Using file encryption where possible, sending passwords/keys via alternative communication channels
- Alerting ICT Services/DPO to any breaches, malicious activity, or suspected frauds

Training

Colchester County High School for Girls recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated frauds.

System Security

ICT Services will build security principles into the design of IT services for Colchester County High School for Girls.

- Security patching – network hardware, operating systems, and software. To be completed within 14 days of a release of a patch where the vulnerability is described as high risk or has a CVSS score of 7 or above.
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them.
- Actively manage anti-virus systems and to ensure that the software is set up to scan files upon access, when downloaded, opened, or accessed from a network folder. Any malicious software is automatically quarantined, and the device cleaned, notifications sent when this has been detected.
- Use software to scan webpages before accessing to ensure the reputation and not phishing or malware sites.
- Actively manage and test backups

- Regularly review and update security controls that are available with existing systems.
- Segregate wireless networks used for visitors' & staff personal devices from school systems.
- Review the security risk of new systems or projects.
- Changing any default password for any device used
- Physically secure or have other control in place for any device that is in public areas that has the potential for theft.
- Maintain a list of approved software and ensure any application deployed is digitally signed and if applicable, is licensed for use.
- Centrally manage application deployment after testing and approving the application.
- Unsupported devices must only access segmented areas of the network which do not grant access to sensitive data.
- Training for all staff who need access to the network will under cyber security training annually. This includes at least one governor.
- Training for technical staff on cyber security will be undertaken annually.

Major Incident Response Plan

Colchester County High School for Girls will develop, maintain, and regularly test a Cybersecurity Major Incident Response Plan. This will include identifying or conducting:

- Key decision-makers
- Key system impact assessments and restoration priorities (i.e., which backups needs to be restored first for the school to become operational again)
- Emergency plans for the school to function without access to systems or data.
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how.
- Key agencies for support (e.g., IT support company)

Any cyber-attacks must be reported to the leadership team. Appropriate action and information-sharing must be conducted in accordance with the General Data Protection Regulation (GDPR). These incidents should also be reported to the DfE sector cyber team at Sector.Incidentreporting@education.gov.uk, and to Action Fraud on the Action Fraud website. Where the incident causes long term school closure, the closure of more than one school or serious financial damage, we will also inform the National Cyber Security Centre.

Maintaining Security

Colchester County High School for Girls understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems. Colchester County High School for Girls will budget appropriately to keep cyber related risk to a minimum.

Appendix 17 – Visitors Acceptable Use Policy

Acceptable Use Policy (AUP) for School Visitors

Welcome to Colchester County High School for Girls. To ensure a safe and secure environment for all users, we ask that you adhere to the following guidelines when using our guest wireless network or a supplied guest access user account.

1. General Use

- Authorisation: Access to the guest wireless network or guest user account is provided for authorised visitors only. Unauthorised use is strictly prohibited.
- Purpose: The network is intended for educational and general internet access and should not be used for any illegal or inappropriate activities.

2. Security and Privacy

- Personal Information: Do not share personal or sensitive information over the network unless it is through a secure, encrypted connection.
- Device Security: Ensure your device has up-to-date antivirus software and security patches installed.
- Network Security: Do not attempt to bypass or interfere with network security measures.
- Account Details: The username and password provided for guest access are for your use only. Do not share these details with anyone else.
- Wireless Password: The guest wireless password is for your use only. Do not share this password with anyone else.

3. Prohibited Activities

- Illegal Activities: Do not engage in any activities that are illegal under UK law.
- Inappropriate Content: Accessing, downloading, or distributing inappropriate or offensive content is prohibited.
- Network Misuse: Activities that disrupt or degrade the performance of the network, such as excessive bandwidth usage or spreading malware, are not allowed.
- Respectful Use: Ensure that your use of the network is respectful and appropriate, particularly in a school environment.

4. Monitoring and Compliance

- Monitoring: The school reserves the right to monitor network activity to ensure compliance with this policy.
- Compliance: Failure to comply with this AUP may result in the termination of network access and potential legal action.

5. Device Support, Requirements, and Responsibility

- Responsibility: Users are responsible for their actions while connected to the network. The school is not liable for any damages or losses resulting from network use.

- Technical Support: Technical support will be limited to connecting the device to the guest wireless network only for devices not owned by Colchester County High School for Girls.
- Minimum Requirements: The school reserves the right to reject requests for access to the guest wireless network if the device doesn't meet required minimum hardware and software requirements.
- For any support, questions or guidance, please ask any member of staff or contact ICT Services on 8008 or ask a member of staff to contact ICT Services on your behalf.

By using the guest wireless network or guest access user account, you agree to abide by this Acceptable Use Policy. Thank you for your cooperation.