Policy Title	**eSafety and Data Security**
Author	**W Jenkins**
Linked to *(and should be applied in conjunction with)* the College's policies on:	**Data Protection and Freedom of Information policy** **Child Protection Policy**

Equality Impact Assessment

The EIA has not identified any potential for discrimination or adverse impact and all opportunities to promote equality have been taken.*	✓
The EIA has not identified any conflict with the College's co-operative values.	✓
Adjust the policy to remove barriers identified by the EIA or better promote equality.	

*Inclusive of protected characteristics

CONTENTS

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Helston Community College, we understand the responsibility to educate our students on eSafety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Our College holds personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the College. This can make it more difficult for us to use technology to benefit learners.

Everybody in the College has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and students) are inclusive of both fixed and mobile internet; technologies provided by the College (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto College premises (such as laptops, mobile phones and other mobile devices).

The staff responsible for monitoring and advising on this policy are:

Wayne Jenkins	Deputy Headteacher with responsibility for eSafety and Data Protection
Frank Mathieson	Network Manager with responsibility for ICT infrastructure
Laura Hocking	eSafety Co-ordinator
David Lewis	AHT with responsibility for safeguarding and child protection

Monitoring

Authorised ICT staff may inspect any ICT equipment owned by the College at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please contact the network manager.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain College business related information; to confirm or investigate compliance with College policies, standards and procedures; to ensure the effective operation of College ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

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

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

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

At Helston Community College we use specialist e-Safety monitoring software provided by Future Digital. This is currently installed and monitoring is active and ongoing. The software allows the freedom to use the internet and computer programs responsibly, whilst capturing misuse and unacceptable behaviour.

The software detects potentially inappropriate content as soon as it appears on screen or is typed in by the user. A screen capture is taken of every incident detailing the time and date of capture, machine name, user name and reason for capture. A weekly headline summary is produced from the system detailing captures of particular interest and automatically emailed to a small number of selected staff who monitor the system. These particular violations will be investigated and dealt with in accordance with our Acceptable Use Policy, Behaviour Policy, e-Safety, Anti-Bullying, Safeguarding and any other relevant College policies.

We are alerted to students using threatening behaviour or accessing inappropriate websites for example. It also gives an early warning of potentially harmful situations, like predator grooming or radicalisation threats. The captured evidence helps staff choose the best course of action, from support for victims of bullying, or protecting a vulnerable child, to confronting a student who is acting inappropriately. The monitoring software also provides a powerful incentive for students to use all technology and devices safely and concentrate in lessons. Learning good habits at College prepares children for a continued safe digital future.

Breaches

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

For staff, any policy breach is grounds for disciplinary action in accordance with the College Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Students who breach this policy will be sanctioned in accordance with the College's behaviour policy.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the College's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the College are as follows: Frank Mathieson (Network Manager), Laura Hocking (eSafety Co-ordinator) and Wayne Jenkins (Deputy Headteacher).

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

Acceptable Use Agreement: Students

- I will only use ICT systems in College, including the internet, e-mail, digital video, and mobile technologies for College purposes
- I will not download or install software on College technologies
- I will only log on to the College network, other systems and resources with my own user name and password
- I will follow the College's ICT security system and not reveal my passwords to anyone and change them regularly
- I will only use my College e-mail address
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
- I will be aware of "stranger danger" when I am communicating on-line and I will not disclose or share personal information about myself or others, such as name, phone number or address.
- I am aware that when I take images of students and/ or staff, that I must only store and use these for College purposes in line with College policy and must never distribute these outside the College network without the permission of all parties involved. This includes educational visits and all occasions when I am in College uniform or when otherwise representing the College
- I will ensure that my online activity, both in College and outside College, will not cause my College, the staff, students or others distress or bring the College community into disrepute, including through uploads of images, video, sounds or texts
- I will support the College approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the College community
- I will respect the privacy and ownership of others' work on-line at all times
- I will not attempt to bypass the internet filtering system
- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in College if I have permission. I understand that, if I do use my own devices in College, I will follow the rules set out in this agreement, in the same way as if I was using College equipment.
- I understand that the College will not accept responsibility for the loss or damage of my personal electronic devices which I choose to bring on site.
- I understand that all my use of the Internet and other related technologies will be monitored and logged and can be made available to my teachers
- I understand that these rules are designed to keep me safe and that if they are not followed, College sanctions will be applied and my parent/ carer may be contacted. I also understand that in the case of illegal activities, the police will be involved.

Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in College. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to read and agree to this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Deputy Headteacher.

- I will only use the College's email / Internet / Intranet / Google Apps and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the College or other related authorities
- I will ensure that all electronic communications with students and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to students
- I will only use the approved, secure e-mail system for any College business
- I will ensure that personal data (such as data held on SIMS software) is kept secure and is used appropriately, whether in College, taken off the College premises or accessed remotely. Personal data can only be taken out of College or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted and stored on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the network manager
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line with College policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the College network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the College approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the College community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in College and outside College, will not bring the College, my professional role or that of others into disrepute
- I will support and promote the College's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies

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

College ICT Equipment

- As a user of the College ICT equipment, you are responsible for your activity
- The College logs ICT equipment issued to staff and records serial numbers as part of the College's inventory
- Do not allow your visitors to plug their ICT hardware into the College network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the College's network. You are responsible for the backup and restoration of any of your data that is not held on the College's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- A time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on the College network, but access the internet through the College Wi-Fi is allowed at the discretion of the Deputy Headteacher
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the Network Manager. The Network Manager is responsible for:
    - maintaining control of the allocation and transfer to the member of staff
    - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

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

personal or sensitive data

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

Mobile Technologies

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

Personal Mobile Devices (including phones), often referred to as BYOD (Bring Your Own Device)

- The College allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the College allow a member of staff to contact a student using their personal device.
- Students are allowed to bring personal mobile devices/phones to College but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent
- Staff who wish to set up and use a College e-mail account on their personal mobile device will need to have some form of device locking e.g. password or pin. If the device gets lost

or stolen, the Network Manager needs to be informed as soon as possible so that the device can be remotely wiped of data.

- This BYOD technology may be used for educational purposes but the class teacher should agree the activity with the Deputy Headteacher or e-Safety Co-ordinator.

- Decisions regarding access to the College Wi-Fi system will be made by the Deputy Headteacher and decisions will be final and binding.

- Students and staff using personal mobile devices on the College Wi-Fi system are subject to internet filtering and expected to abide by the AUAs they have signed or agreed to electronically.

- The College is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text or instant messages between any member of the College community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the College community

- Users bringing personal devices into College must ensure there is no inappropriate or illegal content on the device

College Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the College community is not allowed

- Permission must be sought before any image or sound recordings are made on the devices of any member of the College community

- Where the College provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used

- Where the College provides a laptop for staff, this device should only be used for College business

- Never use a hand-held mobile phone whilst driving a vehicle

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using College provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on College ICT equipment.

- If your machine is not routinely connected to the College network, you must make provision for regular virus updates through the ICT technical team.

- If you suspect there may be a virus on any College ICT equipment, stop using the equipment and contact the ICT technical team immediately. The ICT technicians will advise you what actions to take and be responsible for advising others that need to know.

Data Security

The accessing and appropriate use of data is something that the College takes very seriously.

Security

- The College gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are made aware of their responsibility when accessing College data
- Staff have been issued with the relevant data protection policy documents and the Policy for ICT Acceptable Use
- The Headteacher has identified relevant responsible persons for managing data security
- Staff must keep all College related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared multi-function print, fax, scan and copiers are used. These devices are password protected to minimize risk.

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the College's response. The Deputy Headteacher has the following responsibilities:

- lead on information risk assessment
- advise College staff on the appropriate use of information systems
- make sure that information handling complies with legal requirements

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. SLT should be able to identify across the College:

- what information is held, and for what purposes
- what information needs to be protected, how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

However, it should be clear to all staff that the handling of secure data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen

- Disposal of any ICT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations 2006
  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
  http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
  http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

  Data Protection Act 1998
  https://ico.org.uk/for-organisations/education/
  Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The College will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

- The College's disposal record will include:

  - Date item disposed of
  - Authorisation for disposal, including:
    - verification of software licensing
    - any personal data likely to be held on the storage media? *
  - How it was disposed of eg waste, gift, sale
  - Name of person & / or organisation who received the disposed item

* if personal data is likely to be held, the storage media will be over written multiple times to ensure the data is irretrievably destroyed. We may also choose to physically destroy the storage media to reduce risk further.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

e-mail

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

Managing e-mail

- The College gives all staff & governors their own e-mail account to use for all College business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- Staff & governors should use their College email for all professional communication.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The College email account should be the account that is used for all College business

- Under no circumstances should staff contact students, parents or conduct any College business using personal e-mail addresses

- The College requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the College'. The responsibility for adding this disclaimer lies with the network manager and will automatically be added as a footer. This disclaimer must not be edited or deleted by the account holder

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on College headed paper

- E-mails created or received as part of your College job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

  - Delete all e-mails of short-term value
  - Do not use the e-mail application as a data and file storage system
  - E-mails that need to be kept should be identified for content and filed appropriately
  - Organise e-mail into folders and carry out frequent house-keeping on all folders, retaining emails for a maximum of 18 months

- Staff must inform (the eSafety co-ordinator or line manager) if they receive an offensive e-mail

- However you access your College e-mail, (whether directly, through webmail when away from the office or on personal hardware) all the College e-mail policies apply

- Students may only use College approved accounts on the College system and only under

direct teacher supervision for educational purposes

- All student e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

- Students must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail

- Students are introduced to e-mail as part of the Computing Programme of Study

Sending e-mails

- Use your own College e-mail account so that you are clearly identified as the originator of a message. Having a clearly defined subject line helps the recipient to sort the email on receipt. A clear subject line also assists in filing all emails relating to individual projects in one place.

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain emails. If you send a message externally to more than one person, you must hide the recipients' email addresses. You can do this by putting just your own name in the "To" field, and putting the other addresses in the "Bcc" field.

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

- College e-mail is not to be used for personal matters, including personal business, disputes or legal affairs, nor state views that may be libelous or detrimental to the reputation of the College

- Whenever possible, omit personal identifiable data such as names, date of birth, address etc. from any emails. When referring to students in emails use their initials in the 'subject' of the email and not their full name.

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section:

- e-mailing Personal, Sensitive, Confidential or Classified Information

Receiving e-mails

- Check your e-mail regularly

- Activate your 'out-of-office' notification when away for extended periods

- Never open attachments from an untrusted source; consult your network manager first

- Do not use the e-mail systems to store attachments. Where the main purpose of the email is to transfer documents, then the documents should be saved into the appropriate places in an electronic filing system or printed out and added to a paper file. The email can then be deleted.

- When receiving an email containing personal identifiable information about a student, parent/carer or member of staff, the email is classified as a record which must be dealt with appropriately under data protection guidelines. In these cases, print off a hard copy and place in the appropriate student or staff file and retain in line with the records retention schedule.

- The automatic forwarding and deletion of e-mails is not allowed. Do not set up rules to automatically forward your College e-mail to a personal e-mail account for example.

---

e-mailing Personal, Sensitive, Confidential or Classified Information

- Where your conclusion is that e-mail must be used to transmit such data:

  Obtain express consent from your line manager to provide the information by e-mail and <u>exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:</u>

  - Encrypt and password protect. See the Network Manager on how to do this.
  - Verify the details, including accurate e-mail address, of any intended recipient of the information
  - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
  - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

Equal Opportunities

Students with Additional Needs

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

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

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

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the College, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this College is Laura Hocking, who is line managed in this role by the Deputy Headteacher. All members of the College community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Cornwall LA, CEOP (Child Exploitation and Online Protection) and Childnet.

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

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

eSafety in the Curriculum

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

- The College has a framework for teaching internet skills in Computing lessons
- The College provides opportunities within tutorials and PSHCE days to teach about eSafety
- Educating students about the online risks that they may encounter outside College is done informally when opportunities arise and as part of the eSafety curriculum
- Students are made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Students are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button
- Students are taught to critically evaluate materials and learn good searching skills through the Computing curriculum and through general research opportunities in other subjects.

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety and how they can promote the ‘Stay Safe’ online messages in the form of tutorial resources, staff meetings and briefings and the staff bulletin

- New staff receive information on the College’s acceptable use policy as part of their induction

- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the College community (see eSafety Co-ordinator)

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the College eSafety Messages

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

- The key messages in the eSafety policy will be introduced to the students at the start of each academic year

- eSafety posters will be prominently displayed

- The key eSafety advice will be promoted widely through College displays, website, newsletters, class activities and so on

- We will participate in Safer Internet activities during PSHCE days.

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the College's relevant responsible person or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access passwords), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Deputy Headteacher.

eSafety Incident Log

Keeping an incident log is an effective way of monitoring what is happening and identify trends or specific concerns. This is kept by the Deputy Headteacher.

'Helston Community College' **eSafety Incident Log**

Details of ALL eSafety incidents to be recorded by the eSafety Coordinator. This incident log will be monitored termly by the Headteacher, Member of SLT or Chair of Governors. Any incidents involving Cyberbullying may also need to be recorded elsewhere

Date & time	Name of student or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Misuse and Infringements

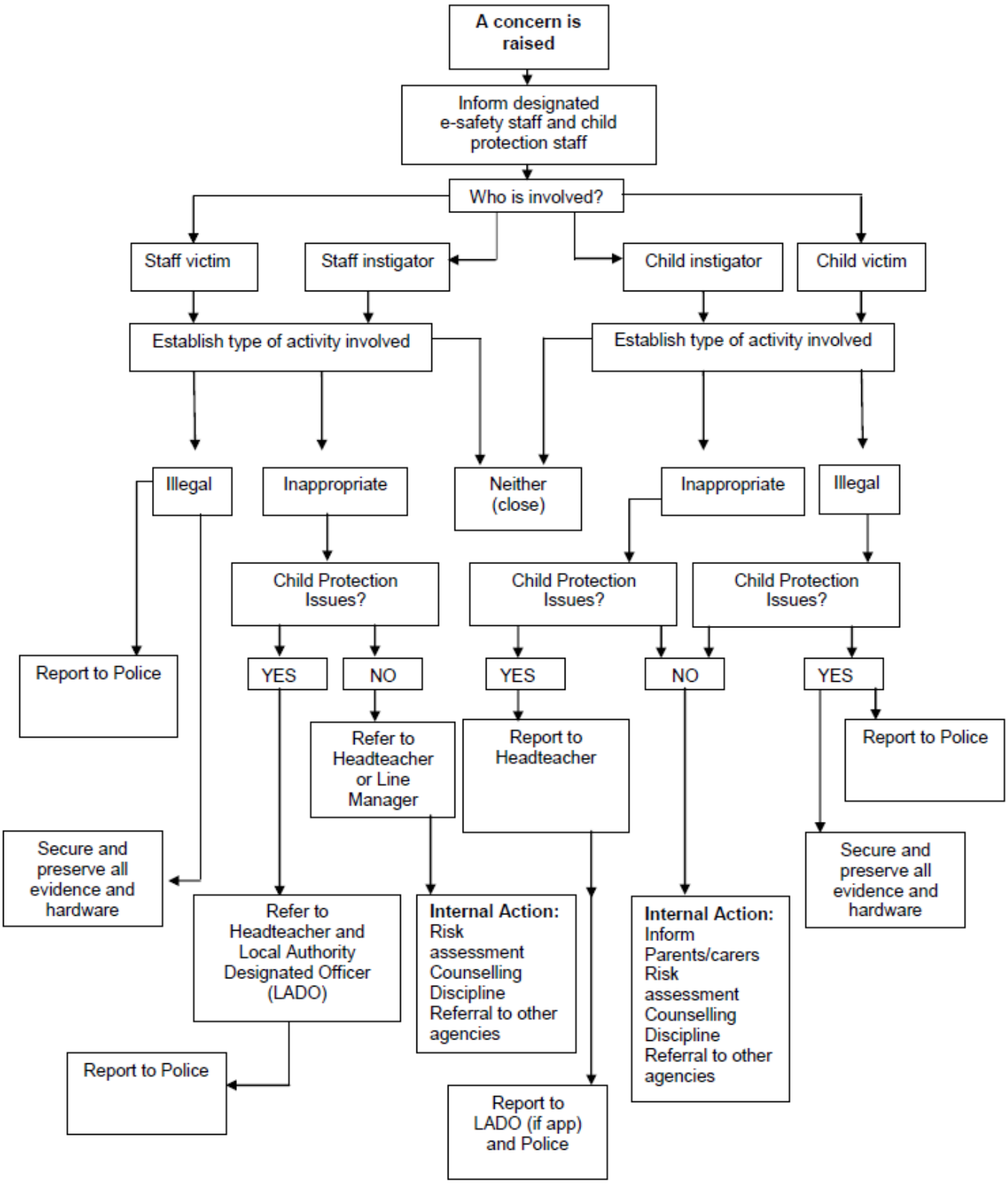
Complaints

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Deputy Headteacher. Incidents should be logged and the **Flowcharts for Managing an eSafety Incident** should be followed.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator or Deputy Headteacher
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation co-ordinated by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct through login information messages and the staff guide

Managing an eSafety Incident



Other Incidents

It is hoped that all members of the College community will be responsible users of digital technologies, who understand and follow College policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action

If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of ‘grooming’ behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the College and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

College Actions & Sanctions

It is more likely that the College 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 College 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.

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through the College network is logged and Future Digital software continually monitors for any inappropriate use, taking screenshots of such activity. Whenever any inappropriate use is detected it will be followed up and logged.

Managing the Internet

- The College provides students with filtered and supervised access to Internet resources (where reasonable) through the College's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is potentially risky; checks should be carried out beforehand by the teacher and guidance on appropriate search terms and techniques should be provided to students
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher
- All users must observe software copyright at all times. It is illegal to copy or distribute College software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, students, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or non-educational gaming is not allowed in College
- Social networking is not allowed in College other than the College's official Facebook page and Twitter feeds (exceptions may be agreed with the eSafety co-ordinator for educational purposes related to eSafety)

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

Infrastructure

- College internet access is provided by BT
- Our College uses web-filtering which is the responsibility of the Network Manager
- Helston Community College is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and students are aware that College based email and internet activity is actively monitored and explored further if required
- The College uses management control tools for controlling and monitoring workstations
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator, network manager or teacher as appropriate
- It is the responsibility of the College, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all College machines
- Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the College's responsibility nor the network manager's responsibility to install or maintain virus protection on personal systems. If students or staff are concerned about possible infection of their removable media it must be given to the technician for a safety check first
- Students and staff are not permitted to download programs or large files on College based technologies without seeking prior permission from network manager
- If there are any issues related to viruses or anti-virus software, the network manager should be informed as soon as possible

Managing Other Online Technologies

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

- At present, the College endeavors to deny access to social networking and online games websites to students within College
- All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our students are asked to report any incidents of Cyberbullying to the College
- Staff may only create blogs, wikis or other online areas in order to communicate with students using systems approved by the Deputy Headteacher
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

Parental Involvement

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

- Parents/carers are actively encouraged to contribute to adjustments or reviews of the College eSafety policy through parent voice activities

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the College

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (eg, on the College website)

- The College disseminates information to parents relating to eSafety where appropriate in the form of;

    - Information evenings
    - Practical training sessions eg current eSafety issues
    - Leaflets
    - College website information
    - Newsletter items

Passwords and Password Security

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords private and not to share with others, particularly their friends. Visitors such as supply staff and student teachers are given a particular 'Cover' or 'Trainee' username and password, with suitable access rights. These areas are checked, files deleted and passwords changed as appropriate.

Staff and students are regularly reminded of the need for password security.

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Passwords must contain a minimum of six characters and be difficult to guess
- Password changes will be enforced every term for staff
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on loose paper or in an unprotected file
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a child or colleague your password**
- **If you aware of a breach of security with your password or account inform the network manager immediately**
- Passwords for staff and students who have left the College are changed immediately and their accounts are subsequently removed from the system

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

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

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

- Ensure removable media is purchased with encryption or consult with the IT Technicians who will be able to install encryption software
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to College systems, keep all dial-up access information such as logon IDs, passwords and additional passphrase confidential and do not disclose them to anyone
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect College information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-College environment

Safe Use of Images

Taking of Images and Film

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

- With the written consent of parents (on behalf of students) and staff, the College permits the appropriate taking of images by staff and students with College equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However, with the express permission of the Deputy Headteacher, images can be taken provided they are transferred immediately and solely to the College's network and deleted from the staff device
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Deputy Headteacher
- Staff must check image permissions recorded in SIMS before any image can be uploaded for publication
- On occasions it may be suitable to seek separate permissions for certain events such as trips and visits and where media organisations may be present for example.

Consent of Adults Who Work at the College

- Permission to use images of all staff who work at the College is sought on induction and a copy is located in the personnel file

Publishing Student's Images and Work

On a child's entry to the College, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the College web site and Facebook page
- in the College prospectus and other printed publications that the College may produce for promotional purposes
- in promotional videos and CDs
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this College unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the College.

Students' names will not be published alongside their image unless permission has been given. Students' full names will not be published unless permission has been given. E-mail and postal addresses of students will not be published.

Only a small number of staff have access to College approved internet systems and the appropriate authority to upload to the internet. Uploading names and/or images to unofficial systems is not permitted and could result in disciplinary action.

Storage of Images

- Images/ films of children are stored on the College's network and within the College's Google Apps for Education environment
- Students and staff are not permitted to use personal portable media for storage of images (eg, USB sticks) without the express permission of the Deputy Headteacher
- Rights of access to this material are restricted to the teaching staff and students within the confines of the College network or Google Apps
- The relevant staff who uploaded the images have the responsibility of deleting the images when they are no longer required, or within one year of the student leaving the College.

Webcams and CCTV

- The College uses CCTV for security and safety. The only people with access to this are the Network Manager and the senior leadership team. Notification of CCTV use is displayed at the front of the College. Please refer to the hyperlink below for further guidance https://ico.org.uk/about-the-ico/consultations/cctv-code-of-practice-revised/
- We do not use publicly accessible webcams in College
- Webcams will not be used for broadcast on the internet without prior parental consent
- Misuse of the webcam by any member of the College community will result in sanctions (as listed under the 'inappropriate materials' section of this document)
    - Webcams can be found around the College site. Notification is given in the areas filmed by webcams by signage
    - Parents/carers and staff are notified of the use of CCTV in the relevant Privacy Notice

- Webcams include any camera on an electronic device which is capable of producing video. College policy should be followed regarding the use of such personal devices

---

Video Conferencing

This type of activity takes place very rarely. If students are involved:

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the College
- All students are supervised by a member of staff when video conferencing
- The College keeps a record of video conferences, including date, time and participants
- Approval from the Deputy Headteacher is sought prior to all video conferences within College to end-points beyond the College
- No part of any video conference is recorded in any medium without the written consent of those taking part

Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine’s specification
- Data must be backed up regularly on a separate server located in a different building

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our College uses Facebook and Twitter to communicate with parents and carers. A small College communications team is responsible for all postings on these technologies and monitors responses from others

- Staff ***are not*** permitted to access their personal social media accounts using College equipment at any time

- Selected ICT staff are able to setup Social Learning Platform accounts, using their College email address, in order to be able to teach students the safe and responsible use of social media

- Students are not permitted to access their social media accounts on College equipment or through College Wi-Fi.

- Staff, governors, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others

- Staff, governors, students, parents and carers are made aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

- Staff, governors, students, parents and carers are made aware that their online behaviour should at all times be compatible with UK law

- Staff must not post inappropriate comments on social media about students, parents, colleagues or the College in general. Staff are required to uphold the reputation of the College, to maintain reasonable standards in their own behaviour, and to uphold public trust in the profession. Bringing the College or your profession into disrepute will result in disciplinary action, possibly leading to dismissal.

- If staff experience online abuse from students or parents, it is important not to retaliate i.e. personally engage with cyberbullying incidents. Keep any records of abuse – texts, emails, voice mails, or instant messages. Take screen prints of messages or web pages. Record the time, date and address of the site. Inform the Headteacher at the earliest opportunity so that the matter can be dealt with appropriately.

Systems and Access

- You are responsible for all activity on College systems carried out under any access/account rights assigned to you, whether accessed via College ICT equipment or your own devices
- Do not allow any unauthorised person to use College ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from College ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the College or may bring the College into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the College's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on College systems, hardware or used in relation to College business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Writing and Reviewing this Policy

Staff and Student Involvement in Policy Creation

- Staff, governors and students have been involved in making/ reviewing the Policy for ICT Acceptable Use through staff meetings, governor meetings and student council/digital leader meetings

Review Procedure

There will be on-going opportunities for staff to discuss with the eSafety coordinator any eSafety issue that concerns them.

There will be on-going opportunities for staff to discuss with the Deputy Headteacher any issue of data security that concerns them.

There will several opportunities for students to feed back and contribute to the review of this policy through student council and digital leaders meetings.

This policy will be reviewed every 2 years by SLT and Governors and consideration will be given to the implications for future whole College development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998

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

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

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

Regulation of Investigatory Powers Act 2000

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

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

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

Sexual Offences Act 2003

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

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

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

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

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

Malicious Communications Act 1988 (section 1)

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

Copyright, Design and Patents Act 1988

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

Public Order Act 1986 (sections 17 – 29)

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

Protection of Children Act 1978 (Section 1)

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

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

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

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

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/