



ICT Policy

Revised: September 2022

Next review: September 2024

This policy is presented in HTML to support accessibility needs and to work across platforms. This webpage is also printable.

This policy was approved by governors: October 2022

The policy is to be reviewed by: October 2024

ICT is 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, we 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
- Online classrooms such as Google Classroom
- Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

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.

At Cedars Academy, 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.

The Academy holds personal data on learners, staff and other people 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 Academy. This can make it more difficult for the Academy to use technology to benefit learners.

Everybody in the Academy 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, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the Academy (such as PCs, laptops, Chromebooks, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto Academy premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

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

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

Breaches

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

Any policy breach is grounds for disciplinary action in accordance with the Academy Disciplinary Procedure Policy breaches may also lead to criminal or civil proceedings.

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 Academy's eSafety Co-ordinator/DSL, Head of School/College. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Line Manager.

Data Security

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

The Academy follows Becta guidelines [Becta Academies - Leadership and management - Security - Data handling security guidance for Academies](#) (published Spring 2009) and the Local Authority guidance documents listed below

GDPR, data protection and Freedom of Information (FOI)

Security

- The Academy gives relevant staff access to its Management Information System, with a unique ID and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing Academy data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff have read the relevant guidance documents available on the Trust website concerning 'Safe Handling of Data'
- Staff keep all Academy 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 copiers (multi-function print, fax, scan and copiers) are used

Impact Levels and Protective Marking

- Appropriate labelling of data should help Academies secure data and so reduce the risk of security incidents
- Most learner or staff personal data will be classed as Protect
- Protect and caveat classifications that Academies may use are;
- Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business
- Applying too low a protective marking may lead to damaging consequences and compromise of the asset
- The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents

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

Senior Information Risk Owner (SIRO)

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

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs) (these will be Academy Managers who have specific responsibility for the Academy MIS, ICT, safety etc)
- they act as an advocate for information risk management

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Academies should identify an Information Asset Owner. For example, the Academy's Management Information System (MIS) should be identified as an asset and should have an Information Asset Owner. In this example the MIS Administrator or Manager could be the IAO.

The role of an IAO is to understand:

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

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

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

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 overwritten 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:

Waste Electrical and Electronic Equipment (WEEE) Regulations 2013 <https://www.hse.gov.uk/waste/waste-electrical.htm>
Data Protection Act 2018 <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

- The Academy will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The Academy'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 e.g. 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 overwritten multiple times to ensure the data is irretrievably destroyed.

- 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

Further information available at:

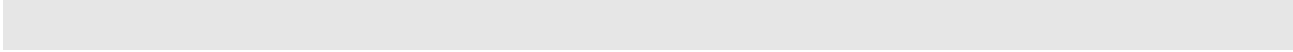
Waste Electrical and Electronic Equipment (WEEE) Regulations

Health and Safety Executive (HSE) [website](#)

<https://www.hse.gov.uk/waste/waste-electrical.htm>

Information Commissioner website

<http://www.ico.gov.uk/>



e-Mail

The use of e-mail within the Academy is an essential means of communication for both staff and students. In the context of Academy, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between institutions on different projects, be they staff based or student based, within Academy or international. We recognise that students need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT Level 4 or above, students must have experienced sending and receiving e-mails.

Managing e-Mail

- The Academy gives all staff and students their own e-mail account to use for all Academy business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- 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 Academy email account should be the account that is used for all Academy business
- Under no circumstances should staff contact students, parents or conduct any Academy business using personal e-mail addresses
- The Academy requires a standard disclaimer to be attached to all e-mail correspondence, stating that; 'the views expressed are not necessarily those of the Academy or the Sponsor'. The responsibility for adding this disclaimer lies with the account holder
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on Academy headed paper
- Staff sending e-mails to external organisations, parents or students are advised to cc. the Principal, line manager or designated account
- Students may only use Academy approved accounts whilst inside the Academy and only under direct teacher supervision for educational purposes
- E-mails created or received, as part of your Academy job will be subject to disclosure in response to a request for information under the GDPR Regulations. You must therefore actively manage your e-mail account as follows:
 - Delete all e-mails of short-term value
 - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All students have their own individual Academy issued accounts
- All student e-mail users are expected to adhere to the generally accepted rules of netique

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 e-mail
- Staff must inform (the eSafety co-ordinator/ DSL/line manager) if they receive an offensive e-mail
- Students are introduced to e-mail as part of the ICT Scheme of Work
- However, you access your Academy e-mail (whether directly, through webmail when away from the office or on non-Academy hardware) all the Academy e-mail policies apply

Sending e-mails

- 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
- Use your own Academy e-mail account so that you are clearly identified as the originator of a message
- If you are required to send an e-mail from someone else's account, always sign on through the 'Delegation' facility within your e-mail software so that you are identified as the sender (if available within your software)
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail
- Academy e-mail is not to be used for personal advertising
- When compiling an email please take care with regard to the content and tone of the email. Keep information factual and avoid emotive statements. Do not use block capital letters in emails as this constitutes as a form of shouting at the recipient/s.

Receiving e-mails

- Check your e-mail regularly and when appropriate to do so

- Activate your 'out-of-office' notification when away for extended periods
- Use the 'Delegation' facility within your e-mail software so that your e-mail can be handled by someone else while you are not at work (if available within your software)
- Never open attachments from an untrusted source; Consult our ICT Technicians first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder on the Academy network
- The automatic forwarding and deletion of e-mails is not allowed

e-mailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible

- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted
- Where your conclusion is that e-mail must be used to transmit such data:
 - Obtain express consent from your manager to provide the information by e-mail
 - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
 - 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 anybody/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

In exceptional circumstances, we can make provision for secure data transfers to specific external agencies.

Equal Opportunities

Students with Additional Needs

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

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

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

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the Academy, the Principal and governors have ultimate responsibility to ensure that the policy and practises are embedded and monitored. All members of the Academy community have been made aware of who holds this post. It is the role of the eSafety coordinator to keep abreast of current issues and guidance through organisations such as Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Trustees are updated by the Chief Executive/eSafety coordinator and all governors understand the issues and strategies at our Academy in relation to local and national guidelines and advice.

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

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 Academy has a framework for teaching internet skills in ICT lessons
- The Academy provides opportunities within a range of curriculum areas to teach about eSafety
- Educating students on the dangers of technologies that may be encountered outside of the Academy is done informally when opportunities arise and as part of the eSafety curriculum which is part of Flexible learning mornings.
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities
- Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or an organisation such as Childline or CEOP report abuse button, the introduction of parent mail regarding issues such as cyber bullying, use of social media etc.
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

eSafety Skills Development for Staff

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

Managing the Academy eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
 - The eSafety policy will be introduced to the students at the start of each Academy year
- 

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

eSafety Incident Log

Some incidents may need to be recorded in other places (ClassCharts and/or CPOMS), if they relate to a bullying or racist incident.

Misuse and Infringements

Complaints

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

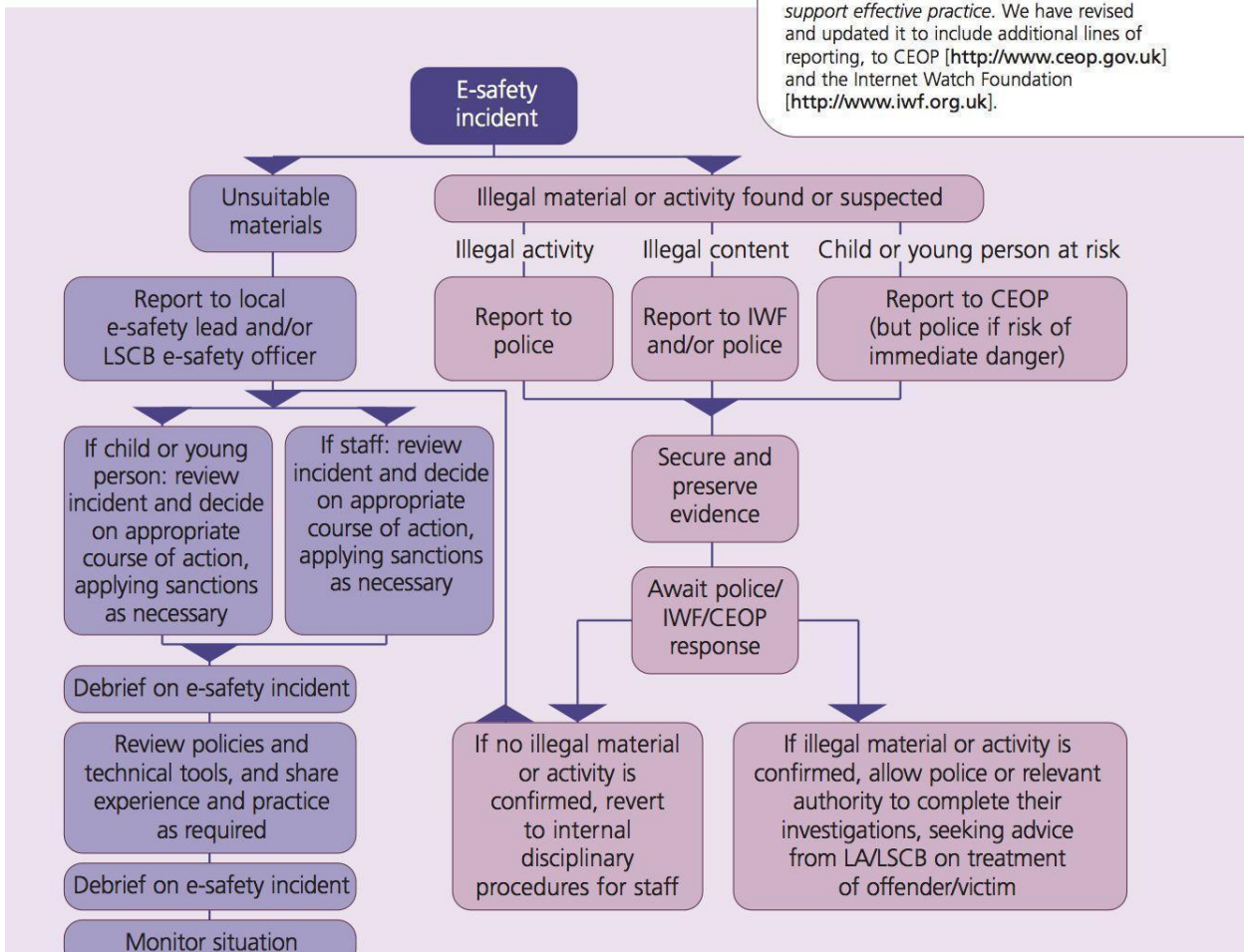
Inappropriate Material

- 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
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Principal and/or Governors, 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 by ***(being issued with a copy of this policy if members of the Academy staff and informed via ICT lessons, assemblies, posters and Learning Tutors)***

Flowchart for Managing an eSafety Incident

appendix B flowchart for responding to e-safety incidents

Note: this flowchart originally appeared as 'Flowchart for responding to internet safety incidents in school' in the Becta publication *E-safety: Developing whole-school policies to support effective practice*. We have revised and updated it to include additional lines of reporting, to CEOP [<http://www.ceop.gov.uk>] and the Internet Watch Foundation [<http://www.iwf.org.uk>].



Internet Access

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

Managing the Internet

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

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience especially on social media websites such as Facebook
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog
- On-line gambling or gaming is not allowed

It is at the Head of School, Services and College's discretion on what internet activities are permissible for staff and students and how this is disseminated.

Infrastructure

- Our Academy employs some additional web filtering which is the responsibility of **the onsite ICT Technicians in conjunction with the 3rd party provider Omnicom Solutions**
- The Academy is aware of its responsibility when monitoring staff communication under current

legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and students are aware that Academy based email and internet activity can be monitored and explored further if required
- The Academy does not allow students access to internet logs
- The Academy 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, teacher or ICT Technicians as appropriate
- It is the responsibility of the Academy, by delegation to the ICT Technician to ensure that Anti-virus protection is installed and kept up-to-date on all Academy 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 Academy's responsibility nor the ICT Technicians' to install or maintain virus protection on personal systems
- Students and staff are not permitted to download programs or files on Academy based technologies without seeking prior permission from the Senior Leadership Group
- If there are any issues related to viruses or anti-virus software, the ICT Technician should be informed via email or phone immediately giving detailed information to assist in remedial action being taken
- Staff must only view videoed IRIS content in secured locations due to the sensitive nature of the video clips.

Managing Other Web Technologies

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 Academy endeavours to deny access to social networking sites to students within Academy
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, Academy details, IM/ email address, specific hobbies/ interests)
- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts online
- Our students are asked to report any incidents of bullying to the Academy
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using Google classroom and the Academy email or other systems approved by the SLG

Parental Involvement

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

- Parents/ carers and students are actively encouraged to contribute to adjustments or reviews of the Academy eSafety policy by a randomly selected questionnaire
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to Academy
- Parents/ carers are required to decide as to whether they consent to images of their child being taken/ used in the public domain (e.g., on Academy website)
- Parents/ carers are expected to sign a Home Academy agreement containing the following statement or similar
 - **We will support the Academy approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the Academy community**
- The Academy disseminates information to parents relating to eSafety where appropriate in the form of;
 - Information and celebration evenings
 - Posters
 - Website/ Virtual Learning Environment postings
 - Newsletter items
 - Bloomz messages

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer-based services
- 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
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to ICT Technician when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Passwords must contain a minimum of six characters and be difficult to guess
- User ID and passwords for staff and students who have left the Academy are removed from the system within 24 hours

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

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 secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the Academy's e-safety Policy and Data Security
- Users are provided with an individual network, email, Virtual Learning Environment and Management Information System (where appropriate) log-in username
- Students are not allowed to deliberately access on-line materials or files on the Academy network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of Academy networks, MIS systems and/or Virtual Learning Environment, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are logged off (or locked where available)
- Due consideration should be given when logging into the Remote Web Access/Outlook Web access to the browser/cache options (shared or private computer)

- In our Academy, all ICT password policies are the responsibility of the ICT Technicians and all staff and students are expected to comply with the policies at all times
-

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the Academy and therefore no longer have authorised access to the Academy's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access. (Further advice available <http://www.itgovernance.co.uk/>)

- Ensure that all user accounts are disabled once the member of the Academy has left
- Prompt action on disabling accounts will prevent unauthorised access
- Regularly change generic passwords to avoid unauthorised access (Microsoft® advise every 42 days)

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any Academy information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-Academy 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 document labelling

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

- Ensure removable media is purchased with encryption
- 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 Academy systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- 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 Academy 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-Academy 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 Academy community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of students) and staff, the Academy permits the appropriate taking of images by staff and students with Academy 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 Principal, images can be taken provided they are transferred immediately and solely to the Academy'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 the others, this includes when on field trips. However, with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the Academy's network and deleted from the student's device

Consent of Adults Who Work at the Academy

- Permission to use images of all staff who work at the Academy 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 Academy, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the Academy website
- on the Academy's Virtual Learning Environment
- in the Academy prospectus and other printed publications that the Academy may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the Academy's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the Academy
- general media appearances, e.g. 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 Academy unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Web Manager has authority to upload to the site.

Storage of Images

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

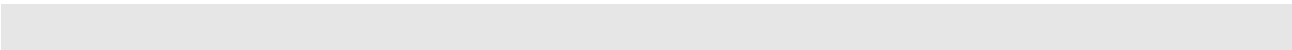
Webcams and CCTV

- The Academy uses CCTV for security and safety. The only people with access to this are the Site Manager, Office Manager and the Senior Leadership Team
- Notification of CCTV use is displayed at the front of the Academy. Please refer to the hyperlink below for further guidance http://www.ico.gov.uk/for_organisations/topic_specific_guides/cctv.aspx
- We do not use publicly accessible webcams in the Academy
- Webcams in Academy are only ever used for specific learning purposes, i.e. monitoring hens' eggs etc
- Misuse of the webcam by any member of the Academy community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
 - Consent is sought from parents/carers and staff on joining the Academy, in the same way as for all images

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the Academy
- All students are supervised by a member of staff when video conferencing
- All students are supervised by a member of staff when video conferencing with end-points beyond the Academy
- The Academy keeps a record of video conferences, including date, time and participants.
- Approval from the Head of School/Services/College is sought prior to all video conferences within Academy
- The Academy conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked
 - Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference
- 

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

Academy ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the Academy's ICT equipment provided to you
- It is recommended that Academy's log ICT equipment issued to staff and record serial numbers as part of the Academy's inventory
- Do not allow your visitors to plug their ICT hardware into the Academy 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 Academy's network drive. You are responsible for the backup and restoration of any of your data that is not held on the Academy's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles. This has been taken off/removed unless you ask for it.
- Privately owned ICT equipment should not be used on a Academy network
- 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 appropriate Line Manager. Authorising Managers are responsible for:
 - maintaining control of the allocation and transfer within their Unit
 - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

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

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

Mobile Technologies

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

Personal Mobile Devices (including phones)

- The Academy allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the Academy allow a member of staff to contact a student or parent/ carer using their personal device
- Students are allowed to bring personal mobile devices/phones to Academy but must not use them for personal purposes within lesson time. At all times the device must be switched onto silent

- This technology may be used, however for educational purposes, as mutually agreed with the Principal. The device user, in this instance, must always ask the prior permission of the bill payer
- The Academy is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the Academy community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the Academy community
- Users bringing personal devices into Academy must ensure there is no inappropriate or illegal content on the device

Academy Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the Academy community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the Academy community
- Where the Academy provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used
- Where the Academy provides a laptop for staff, only this device may be used to conduct Academy business outside of Academy

Removable Media

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media' - Page

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

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
- Back up tapes should be encrypted by appropriate software
- All servers are backed up by first being copied to the Master drive array then to tape according to the following schedule:
 - Differential backups every evening
 - One full backup every Friday

Licensing

It is the responsibility of the Academy/Omnicom Solutions ICT Technicians to ensure all ICT licensing is kept up to date and adhered to.

This includes though is not limited to:

- Windows infrastructure licensing provided through the Microsoft Volume Licensing Service Centre (Windows Server, Microsoft Exchange, Windows, Office etc)
- 3rd Party network administration software (Backup solution, anti-virus etc)
- Any client side applications used on the Academy network

The above information should be kept securely in both digital and wherever possible physical forma

Systems and Access

- You are responsible for all activity on Academy systems carried out under any access/account rights assigned to you, whether accessed via Academy ICT equipment or your own PC
- Do not allow any unauthorised person to use Academy ICT facilities and services that have been provided to you
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from Academy ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the Academy or may bring the Academy or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the Academy'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 Academy systems, hardware or used in relation to Academy 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. *Dell and approved 3rd parties offer this service*

Telephone Services

- You may make or receive personal telephone calls provided:
 1. They are infrequent, kept as brief as possible and do not cause annoyance to others
 2. They are not for profit or to premium rate services
 3. They conform to this and other relevant Academy policies.
- Academy telephones are provided specifically for Academy business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that your incoming telephone calls can be handled at all times
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. Inform the Principal immediately or the Vice Principal designated to deputise in the Principal's absence.

Mobile Phones

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

Writing and Reviewing this Policy

Staff and Student Involvement in Policy Creation

- Staff and students will be involved in reviewing the Policy for ICT Acceptable Use through Academy School/College Council, staff meetings)
-

Review Procedure

There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them

There will be an on-going opportunity for staff to discuss with the SIRO/AIO any issue of data security that concerns them

This policy will be reviewed every (12) months and consideration given to the implications for future whole Academy 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 2018

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

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

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

<http://www.hms0.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 Academy 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.hms0.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hms0.gov.uk/acts/acts1998/19980042.htm>

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

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

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. Academies should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

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

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 their author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

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 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

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx