South Devon UTC e-Safety Policy

Document Control

Version	Date	Author	Notes on Revisions
1.0	14 April 2015	Ian Crews	

Owner	Author	Review	Next review	Approval committee
AP	PL	Annually 06/2015	06/2016	CPLS

CONTENTS

1.1 WHAT IS E-SAFETY?

The UTC's E-Safety Policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for students. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Students must also learn that publishing personal information could compromise their security and that of others. Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to 'groom' children.

Schools can help protect themselves by making it clear to students, staff and visitors that the use of UTC equipment for inappropriate reasons is "unauthorised". However, colleges should be aware that a disclaimer is not sufficient to protect a college from a claim of personal injury and the college needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

1.2 RESPONSIBILITIES OF UTC STAFF

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss E-Safety issues with students. The trust between students and UTC staff is essential to education but very occasionally it can break down. Nationally, CEOP has been set up by the Home Office to "safeguard children's online experiences and relentlessly track down and prosecute offenders". A member of staff who flouts security advice, or uses e-mail or the Internet for inappropriate reasons risks dismissal.

All staff will have signed an ICT Acceptable use policy and accept that the SLT will monitor network and Internet use to help ensure staff and student safety. Support staff that manage filtering systems or monitor ICT use have great responsibility and must be appropriately supervised. Inappropriate or illegal ICT use must be reported to the safeguarding officer. Staff must be aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images to investigate their source. It is recommended that staff follow the following rules before using the internet as a teaching resource:-

- Curriculum Internet use should be planned, task-orientated and educational.

- Staff should guide students in on-line activities that will support the learning outcomes planned appropriate

to the students' age and maturity.

- Students need to know how to cope if they come across inappropriate material including the Report card and the CEOP report button which is available within the My Learning portal.

- E-mail, text messaging and IM all provide additional channels of communication between staff and students and inappropriate behaviour can occur, or communications can be misinterpreted. Where the use of web-based tools supports collaboration, moderation systems are in-place to ensure that inappropriate communication is managed.

Staff might reflect on the power of the technology in police hands to identify the sender of inappropriate messages and phones for staff-student contact should be used to protect staff from false accusations. No member of staff should share their personal details such as phone number even when on an educational visit, the use of UTC mobile phones to contact students is a requisite.

1.3 E-SAFETY FOR STUDENTS WITH ADDITIONAL NEEDS

There is an underlying assumption that children have both understanding and application of "safety". Students need to understand that rules given to them must be followed. Students need to learn safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. Students need to understand that certain rules will change and develop as they get older

Students need to learn how to apply strategies that will help them to avoid certain "risks" such that they need to plan ahead.

There are certain aspects of the above that are particularly challenging for students with additional needs and children who we may consider to be vulnerable in this learning context. Students will clearly have individual needs that will present a range of issues when teaching E-Safety but some common difficulties may be:

- They may be still developing their social understanding of safety and so may relate better to strategies used with younger children

- They are likely to find it hard to apply the same rules in different situations

- Most safety principles rely on children being able to explain what happened or to ask for help

- Some children may have poor recall and difficulties with learning through experience.

- It would seem to be appropriate, therefore, that this policy may need to be adapted to meet the needs of all of our students during an academic year if needs should change.

This may take the form of child-focused strategies that would apply to a student with specific needs and would be made available to all staff involved in Internet use with that child. Alternatively, whole college approaches could take into consideration strategies that would support the needs i.e. specific choices of visual support to remind students of the rules. Advice and guidance can be sought from the safeguarding officer.

1.4 ROUTES TO E-SAFETY

The safe and effective use of the Internet is an essential life-skill, required by all students and staff. Unmediated Internet access brings with it the possibility of placing students in embarrassing, inappropriate and even dangerous situations. This policy aims to ensure responsible ICT use and the safety of students in consultation with staff,

parents, governors and students. The E-Safety Policy will work in conjunction with other policies including Behaviour, Safeguarding and Anti-Bullying.

In writing this E-Safety policy, we have considered these issues:

Guided educational use
Curriculum Internet use produces significant educational benefits including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment in order to enrich and extend learning activities. Directed and successful Internet use will also reduce the opportunities for activities of little education value. Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.

Risk assessment
21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At an appropriate age they will need to learn to recognise and avoid these risks – to become "internet-wise".
We need to perform risk assessments to ensure that our students are fully aware of and can mitigate risks of Internet use. Students need to know how to cope if they come across inappropriate material.
Students may access the Internet in Youth Clubs, Libraries, public access points and in homes. Where possible we will take a lead to help guide staff and parents by offering support and development opportunities.

Responsibility
E-Safety depends on staff, colleges, governors, advisers, parents and - where appropriate - the students themselves taking responsibility. Staff have a particular responsibility to supervise use, plan access and set good examples. The balance between educating students to take a responsible approach and the use of regulation must be judged carefully.

Regulation
The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. In some cases, access must simply be denied, for instance un-moderated chat rooms present immediate dangers and are usually banned. Fair rules, clarified by discussion and prominently displayed at the point of access will help students make responsible decisions.

The IT support technician will keep an up-to-date record of access levels granted to all network users. Parents should be informed that students will be provided with supervised Internet access and parents and students should sign an acceptable use agreement. The Leadership Team Member with overall responsibility for ICT will take responsibility for regularly checking that filtering and monitoring is appropriate, effective and reasonable, and that technical staff have not taken on themselves the responsibility for educational or disciplinary issues. Filtering software is used in place and will provide a level of access to the internet in line with acceptable college use.

Appropriate strategies
This policy describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding students towards educational activities. There are no straightforward or totally effective solutions and staff, parents and the students themselves must remain vigilant. The UTC will take all reasonable precautions to ensure that users access only appropriate material. Filtering strategies will be selected, in discussion with the filtering provider where appropriate. The filtering strategy will be matched to the age and curriculum requirements of the Student.

Principles behind Internet use

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the college's management information and business administration systems. Internet access is an entitlement for students who show a responsible and mature approach to its use. The UTC has a duty to provide students with safe and secure Internet access as part of their learning experience. The UTC's Internet access should be designed expressly for student use and will include filtering appropriate to the age of the student.

Students will be taught what is acceptable and what is not and given clear objectives for Internet use. This will be delivered after staff have received E-Safety training and the teaching materials developed with CEOP's guidance. A proportion of tutor time will be spent teaching the students E- Safety strategies and time allowed for developmental discussion to raise awareness and impart knowledge and understanding.

E-Safety education

Students will be educated in the responsible and safe use of the Internet and other technologies through a range of strategies including:

- Reactive discussion when a suitable opportunity occurs.
- We will ensure that the use of Internet derived materials by staff and by students complies with copyright law, students will be made aware of plagiarism and issues relating to work research being undertaken for coursework. Staff and students will be trained to become critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students will be taught to acknowledge the author of the information used and to respect copyright when using Internet material in their own work.
- Staff and student electronic communications
- Staff and students need to understand that the use of the college's network is a privilege which can be removed should a good reason arise. The college will monitor all network and Internet use in order to ensure student safety.
- Visiting speakers through the SMSC programme.

All users should be expected to adhere to the generally accepted rules of network etiquette (netiquette). These include but are not limited to the following:

Be polite.
Use appropriate language.
Do not use abusive language in your messages to others.
Do not reveal the address, phone number or other personal details of yourself or other users.
Do not use the network in such a way that would disrupt the use of the network by other users.

Illegal activities are strictly forbidden.
Note that e-mail is not guaranteed to be private.
System administrators monitor and have access to all e-mail. Messages relating to or in support of illegal activities may be reported to the authorities.
Laptops, computers and networks should only be used by staff for educational and professional purposes associated with South Devon UTC

Using new technologies in education

New technologies should be examined for educational benefit and a risk assessment carried out before use in college is allowed. New technologies and learning opportunities include:
Mobile phones with the power of a PC may come with Internet, Bluetooth and infrared (IR) connectivity and a camera.

My Learning Virtual Learning Platform
Thinking skills as challenged by games environments and simulations
Internet voice and messaging such as Yammer, Interactive Whiteboard and Skype
Digital story telling involving independence of thought and self-motivation
Podcasting, broadcasting and recording lessons
Digital video
Some of these technologies may disappear, but some will change our world. What is important is to combine the experimental ability of youth with the wisdom of teachers to develop appropriate, effective and safe uses in teaching and learning.

1.5 RESPONSE TO AN INCIDENT OF CONCERN

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of college. However, it is also important to consider the risks associated with the way these technologies can be used.

The E-Safety Policy recognises and seeks to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

These risks to E-Safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to students and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity. Incidents will be dealt with as per the school's discipline policy.

This section will help staff determine what action they can take and when to report an incident of concern to the Safeguarding Officer. Matters can then be handed over to the Children's Safeguards Service or the Police if that becomes necessary.

What does electronic communication include?

- Internet collaboration tools: social networking sites and web-logs (blogs) Internet research: websites, search engines and web browsers
- Mobile phones and personal digital assistants (PDAs) Internet communications: e-mail and IM
- Webcams and videoconferencing Wireless games consoles

What are the risks?

Receiving inappropriate content Predation and grooming
Requests for personal information Viewing 'incitement' sites
Bullying and threats Identity theft
Publishing inappropriate content
Online gambling
Misuse of computer systems
Publishing personal information
Hacking and security breaches Corruption or misuse of data

Implementation and Compliance
No policy can protect students without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences. The following ideas and checks may be implemented:

- The quick audit provided in the Core E-Safety Policies is a good place to start when checking the college's E-Safety readiness.

- How are students reminded of their responsibilities? Displaying posters in rooms with computers is one useful approach.
- Do staff, students and parents know how to report an incident of concern regarding Internet use?
- Where filtering is managed locally, does a senior leader approve the UTC filtering configuration and supervise the staff who manage the filtering system?

2.1 TEACHING AND LEARNING

2.1.1 Why is Internet use important?

The purpose of Internet use in South Devon UTC is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the college's management functions. Internet use is part of the statutory curriculum and a necessary tool for learning.

Internet access is an entitlement for students who show a responsible and mature approach to its use.
The Internet is an essential element in 21st century life for education, business and social interaction. The college has a duty to provide students with quality Internet access as part of their learning experience.
Students use the Internet widely outside college and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.1.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- cultural exchanges between students world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- to learning wherever and whenever convenient.

2.1.3 How can Internet use enhance learning?

The UTC Internet access will be designed expressly for students and staff use and will include filtering appropriate to the age of students.

Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.

Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Staff will be able to access the internet for their own professional development and professional responsibilities associated with their role.

2.1.4 How will students learn how to evaluate content?

South Devon UTC will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law.

Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

2.2 MANAGING INFORMATION SYSTEMS

2.2.1 The maintenance of information system security Local Area Network security:

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations are secured against user mistakes and deliberate actions.
- Servers are located securely and physical access restricted to the IT Support staff directly employed in this team.
- The server operating system is secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices is pro-actively managed.

Wide Area Network (WAN) security:

- All Internet connections are arranged by the UTC to ensure compliance with the security policy.
- Firewalls and switches are configured to prevent unauthorized access.
- The security of the college information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not be used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
- Files held on the college's network will be regularly checked.
- The network manager will review system capacity regularly.

2.2.2 The management of e-mail

- Students may only use approved e-mail accounts.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in college to external personal e-mail accounts is blocked.
- Excessive social e-mail use by students can interfere with learning and may be restricted.
- The college's e-mail system must NOT be used for social use.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on college headed paper.

2.2.3 The management of published content

- The contact details on the website will be the college address, e-mail and telephone number. Staff or students' personal information will not be published.

- The principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website will comply with the college's guidelines for publications including respect for intellectual property rights and copyright.

2.2.4 The publishing of student images

- Images that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of students are electronically published.

2.2.5 The management of social networking and personal publishing

The UTC will block/filter access to social networking sites.

- Newsgroups will be blocked unless a specific use is approved.

Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or college.

Teachers' official blogs or wikis should be password protected and run from the MyLearning VLE. Teachers will be advised not to run social network spaces for student use on a personal basis.

Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.

Students should be encouraged to invite known friends only and deny access to others. Students will be advised not to publish specific and detailed private thoughts.

Staff should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

2.2.6 The management of filtering

Internet access must be appropriate for all members of the college community. Older secondary students, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. The technical strategies being developed to restrict access to inappropriate material fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled-garden or "allow-list" restricts access to a list of approved sites. Such lists inevitably limit students' access to a narrow range of information.
- Dynamic filtering examines web page content or e-mail for unsuitable words. Filtering of outgoing information such as web searches is also required.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
- Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.

.
If staff or students discover unsuitable sites, the URL must be reported to the Network Manager. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the college believes is illegal must be reported to appropriate agencies such as CEOP.
The UTC's filtering strategy will be designed by educators to suit the age and curriculum requirements of our students, advised by engineers.

2.2.7 The management of emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in college is allowed.

- Mobile phones will not be used during lessons or formal college time. The sending of abusive or inappropriate text messages is forbidden.
- The college will investigate wireless, infra-red and Bluetooth communication technologies as they develop.
- Staff will be issued with a college phone where contact with students is required.

2.2.8 The protection of personal data Personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes Adequate, relevant and not excessive Accurate and up-to-date
- Held no longer than is necessary Processed in line with individuals rights Kept secure
- Transferred only to other countries with suitable security measures.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.3 POLICY DECISIONS

2.3.1 The authorisation of Internet access

The college will maintain a current record of all staff and students who are granted access to the college's electronic communications. Students must apply for Internet access individually by agreeing to comply with the Acceptable Use Policy. Parents will be asked to sign and return a consent form for student access.

2.3.2 The assessment of risks

The college will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a UTC computer. The UTC can accept liability for the material accessed, or any consequences resulting from Internet use.

The college will audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

2.3.3 The management of E-Safety complaints

Response to an incident of concern.
Complaints of Internet misuse will be dealt with by the safeguarding officer. Any complaint about staff misuse must be referred to the principal.

- Students and parents will be informed of the complaints procedure.
- Parents and students will need to work in partnership with staff to resolve issues.
- Sanctions within the college discipline policy include:
  - interview/counselling by teaching staff;
  - informing parents or carers;
  - removal of Internet or computer access for a period
  - exclusion
  - discussions will be held with the local Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

2.4 COMMUNICATIONS POLICY

2.4.1 How will the policy be introduced to students?

Many students are very familiar with mobile and Internet use and culture and as students' perceptions of the risks will vary; the E-Safety rules will need to be explained or discussed.
A poster in every room with a computer will remind students of the E-Safety rules at the point of use.
The suggested student and parent agreement form will be attached to a copy of the E-Safety rules. Consideration will be given as to the curriculum place for teaching E-Safety. This may be part of the pastoral programme.

2.4.2 How will the policy be discussed with staff?

All staff will be given the UTC E-Safety Policy and its application and importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Staff training in safe and responsible Internet use and on the college E-Safety Policy will be provided as required.

2.4.3 How will parents' support enlisted?

Parents' attention will be drawn to the college's E-Safety Policy in newsletters, the prospectus and on the South Devon UTC website.

Internet issues will be handled sensitively, and parents will be advised accordingly.

A partnership approach with parents will be encouraged. This will include parent evenings with demonstrations and suggestions for safe home Internet use.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

3.0 E-SAFETY CONTACTS AND REFERENCES

Childline
http://www.childline.org.uk/

Child Exploitation & Online Protection Centre http://www.ceop.gov.uk http://www.thinkuknow.co.uk/

Internet Watch Foundation
http://www.iwf.org.uk/

Kidsmart http://www.kidsmart.org.uk/

NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm
Virtual Global Taskforce – Report Abuse http://www.virtualglobaltaskforce.com/

4.0 LEGAL FRAMEWORK Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:
The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making / distributing indecent images of children, raised the age of the a child to 18 years old;
The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006
This Act makes 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. (Typically, teachers, social workers, health professionals, connexions staff fall into this category of trust).
Any sexual intercourse with a child under the age of 13 commits the offence of rape.
N.B. Colleges should already have a copy of “Children & Families: Safer from Sexual Crime” document as part of their child protection packs.
More information about the 2003 Act can be found at 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.

Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

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 someone else's password to access files);
gain unauthorised access, as above, in order to commit a further criminal act (such as fraud);
or impair the operation of a computer or programme (for example caused by viruses or denial of service attacks).
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 his or her "work" without permission.
The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programme's 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.
It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the 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.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes 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 college 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.