European Union
European
Social Fund

Leicester College

Document No:	**IT001**
Issue No.	**2**
Issue Date:	**2023-08-01**
Renewal Date:	**2026-08-01**
Originator:	**ICTS**
Responsibility:	**Director of IT**

ACCEPTABLE USE OF TECHNOLOGIES POLICY

1. PURPOSE

1.1. This Acceptable Use of Technologies Policy (AUTP) applies without exception to all users of ICT facilities and equipment within Leicester College. This includes staff, students, contractors, and any visitors.

1.2. The purpose of this policy is to provide guidance on the use of network resources which includes the use of any Leicester College technology resources (internal or cloud based, the internet, e-mail, instant messaging, social media, media publications, file transmission and voice/data communications).

1.3. The Policy supports the College in its statutory duty defined in the Counter Terrorism and Security Act 2015 (the 'Prevent Duty') to prevent people being drawn into terrorism.

2. SCOPE

2.1. The policy applies to activities taking place in any location where access to and the use of any of the systems and/or equipment takes place, e.g., mobile devices at home, remote access to any of the Leicester College's data, whether cloud based and/or networked resources.

2.2. The Policy also covers the use of personally owned devices (often referred to as BYOD – Bring Your Own Device) on Leicester College premises and which are connected to any of Leicester College's network.

2.3. All users are expected to make themselves familiar with and be bound by this AUTP. A copy of this Policy can be found on the intranet as well as the College website. A paper copy can also be made available on request.

2.4. This Policy should be read in conjunction with Leicester College's Data Protection Policy (GP002) and E-Communications Policy (HR015).

3. AUTHORISATION

3.1. To use ICT facilities at Leicester College a person must have authorised access to the network. Use of facilities will be deemed to be acceptance of the terms and conditions of this policy.

3.2. It is expected that all users will adhere to password guidelines, in addition to all relevant regulatory and legal requirements.

4. PRIVACY AND MONITORING

4.1. The ICT Services department reserves the right to monitor e-mail, telephone, and any other electronically mediated communications, whether stored or in transit, in line with relevant legislation. Leicester College recognises that users' statutory rights to privacy are not affected by this policy.

4.2. Reasons for such monitoring include but are not limited to:

- Investigate or detect unauthorised use of Leicester College telecommunications systems and ensure compliance with this policy or other Leicester College policies
- Ensure operational effectiveness of services (e.g., to detect viruses or other threats to the systems).
- Prevent a breach of the law or investigate a suspected breach of the law, Leicester College policies or contracts.
- Monitor standards and ensure effective quality control.

4.3. Monitoring may involve (but not exclusively):

- Examining the number and frequency of e-mails.
- Viewing sent or received e-mails from a particular mailbox or stored on any server or media.
- Examining logs of ICT facility usage.
- Monitoring the amount of time spent on the Internet.
- Internet sites visited and information downloaded.

4.4. Where abuse is suspected a more detailed investigation involving further monitoring and examination of stored data may be undertaken.

4.5. Where disclosure of information is requested by the Police (or another law enforcement authority) the request should be directed to the Director of Governance and Policy at dpo@leicestercollege.ac.uk.

4.6. Staff that have access to personal data (as defined under the Data Protection Act 2018) are responsible for ensuring that such data is not made available to unauthorised individuals and that the security of all systems used to access and

manage this data is not compromised. Further detail is set out in the Data Protection Policy.

5. ACCESS CONTROL PROCEDURE

5.1. Leicester College maintains the right to access all data including e-mail accounts of staff members after termination of employment for operational reasons and for the continuing delivery of services.

5.2. Where access is required to any electronic data/e-mails of ex-employees or staff on leave/absence, this must be authorised by the line manager or head of department which must then also be authorised by the Human Resources department and forwarded on to ICT Services by way of e-mail 121@leicestercollege.ac.uk

5.3. Access to more specific data systems is agreed with the departmental manager who are the system owners and maintained by ICT Services.

5.4. The following procedures must be followed:

- A manager or member of staff requiring access to data of an ex-employee or staff on leave/absence must be authorised by their line manager and must be agreed with Human Resources. The Human Resources department must send an authorisation e-mail to ICT Services 121@leicestercollege.ac.uk who will grant the relevant permission(s) to the original requestor.
- Members of staff with access to student data are only granted permission for their own class/departmental data and access is maintained by ICT Services.
- Managers who have line management responsibility are granted permissions by the Human Resources and Payroll department only to view relevant employee information required to perform their task. Where there is a change in line management, changes are made by authorised personnel from the Human Resources and Payroll department.
- All access is withdrawn from all systems and account(s) disabled when a member of staff leaves the organisation.

6. DEFINITIONS OF UNACCEPTABLE USAGE

6.1. Unacceptable use of computers and network resources may be summarised as:

6.1.1. Viewing, creating, displaying, or transmitting material that is fraudulent or otherwise unlawful or inappropriate.
6.1.2. Threatening, intimidating, or harassing employees and students including any message that could constitute bullying or harassment, e.g., on the grounds of sex, race, disability, religion or belief, sexual orientation, or age.
6.1.3. Using obscene, profane, or abusive language.

6.1.4. Using language that could incite hatred against any ethnic, religious, or other minority groups.
6.1.5. Intellectual property rights infringement, including copyright, trademark, patent, design, and moral rights.
6.1.6. Defamation (genuine scholarly criticism is permitted).
6.1.7. Unsolicited advertising often referred to as “spamming.”
6.1.8. Sending e-mails that purport to come from an individual other than the person sending the message using, for example, a forged address.
6.1.9. Attempts to break into or damage computer systems or data held thereon referred to as “hacking.”
6.1.10. Actions or inactions which intentionally or unintentionally cause a breach of Leicester College’s ICT security including but not limited to:
- Aiding the distribution of computer viruses or other malicious software.
- Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised.
- Using the network for unauthorised access.
- The introduction or connection of unauthorised hardware to the Leicester College ICT infrastructure.

6.1.11. Using the ICT facilities to conduct personal commercial business or trading.
6.1.12. Spending an unreasonable amount of time on non-work related sites e.g., social media.

6.2. These restrictions should be taken to mean, for example, that the following activities will normally be considered a breach of policy:

6.2.1. Viewing, downloading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence or other valid permission from the copyright holder.
6.2.2. Distribution or storage by any means of pirated software.
6.2.3. Connecting an unauthorised device to the network, i.e., one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, purchasing policy and acceptable use.
6.2.4. Circumvention of network access control.
6.2.5. Monitoring or interception of network traffic, without permission.
6.2.6. Probing for the security weaknesses of systems by methods such as port-scanning, without permission.
6.2.7. Associating any device to network access points, including wireless, to which you are not authorised
6.2.8. Non-academic/non-business-related activities which generate heavy network traffic, especially those which interfere with others’ legitimate use of ICT services, or which incur financial cost.
6.2.9. Excessive use of resources such as file store, leading to a denial of service to others, especially when compounded by not responding to requests for action.
6.2.10. Frivolous use of ICT suites, especially where such activities interfere with others’ legitimate use of ICT services.

6.2.11. Use of CDs, DVDs, USB, and other storage devices for the purpose of copying unlicensed copyright software, music, etc.
6.2.12. Copying of other peoples' website material without the express permission of the copyright holder.
6.2.13. Use of peer-to-peer and related applications for non-business or non-educational purposes. These include, but are not limited to, Ares, BitTorrent, Direct Connect, Morpheus, KaZaA.

6.3. Staff, students, contractors, and visitors should consider the spirit of the Leicester College ethos when working on Leicester College systems. Any conduct which may discredit or harm Leicester College, its staff or the ICT facilities or can otherwise be considered intentionally unethical is deemed unacceptable.

6.4. Incidents of misuse will be dealt with by Leicester College in accordance or be subject to the disciplinary procedures outlined in the terms and conditions of employment (staff) and disciplinary policy (students). The appropriate level of sanctions will be applied as determined by the nature of the reported misuse.

7. LEICESTER COLLEGE NETWORK USE

7.1. The Leicester College network is not to be used for any of the following purposes:

7.1.1. Viewing, creating, storing, transmitting or deliberate receipt (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images (including pseudo images), data or other material, or any data capable of being resolved into obscene, unlawful, or indecent images or material.
7.1.2. Viewing, creating, storing, or transmitting of material which causes, or is likely to cause, annoyance, revulsion, or needless anxiety to Leicester College, its staff, students, visitors or any third party.
7.1.3. Viewing, creation, or transmission of defamatory, abusive, or other unlawful material in respect of Leicester College, its staff, students, visitors or any third party.
7.1.4. Viewing, storage, or transmission of material in such manner that it infringes the copyright of Leicester College, another person or organisation or which discloses confidential or sensitive information or data relating to Leicester College, its staff, students, contractors, visitors or any third party.
7.1.5. Transmission of unsolicited commercial or advertising material.
7.1.6. Any other act which is considered unlawful in any country where the network is being accessed.
7.1.7. Deliberate activities with any of the following characteristics:
i. Wasting staff effort or networked resources, including the effort of staff involved in the support of these services, including but not limited to.
ii. Corrupting or destroying Leicester College or other users' data.
iii. Manipulating and altering assessments, grades, or transcripts.

iv. Accessing and copying files of other users to obtain an improper advantage.
v. Violating the privacy of Leicester College or other users.

7.1.8. Disrupting the work of other users; using the Leicester College network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment).

7.1.9. Continuing to use an item of networking software or hardware after a request that use cease because it is causing disruption to the correct functioning of Leicester College network.

7.1.10. Other misuse of Leicester College network or networked resources, such as the introduction of viruses, extracting material of others and passing it off as one's own, manipulating material of Leicester College or others to one's own advantage, whether pecuniary or otherwise.

7.1.11. Where the Leicester College network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the Leicester College network.

7.1.12. All the provisions of the Acceptable Use Policy and the Joint Academic Network ("JANET") apply to users of the Leicester College network in addition to the provisions herein.

7.1.13. Users are not permitted to access Leicester College network on behalf of third parties without prior written agreement of Leicester College.

7.1.14. It is beyond the resources and ability of Leicester College to monitor all activities. However, where there is sound reason to suspect unacceptable use as defined above, Leicester College reserves the right to inspect a user's material and use history, including e-mail messages, and at its sole discretion block or edit such material as it sees fit. Furthermore, from time to time, Leicester College may implement technical measures to monitor activity on Leicester College network to ensure compliance with the requirements of this Policy and to carry out tests for research purposes.

7.1.15. Acceptance of the right of Leicester College to take steps to prevent suspected misuse is a condition of access to the Leicester College network.

7.1.16. Any external organisation having a direct link into Leicester College network must take all reasonable steps to ensure compliance with the requirements of this Policy and to ensure that unacceptable use of the Leicester College network does not occur. The external organisation must also accept responsibility for informing its own users of the conditions of use of Leicester College network.

7.1.17. Where necessary, and at the sole discretion of Leicester College, access by an individual or organisation may be withdrawn, either temporarily or indefinitely.

7.1.18. In the event of misuse of Leicester College network, Leicester College reserves the right to exclude access to any external organisation, or employee, or student and in the case of:

i. Misuse by an employee of Leicester College, to proceed against that employee under the Leicester College's disciplinary procedures for employees and
ii. Misuse by a student, to proceed against that student in accordance with the Leicester College's student disciplinary procedures.

7.1.19. Individuals must not share the passwords for any to their Leicester College accounts. Account owners are held responsible for all activities and content associated with their accounts. Failure to conform to these requirements may lead to the suspension of account privileges or other actions as provided by the appropriate Leicester College policy. If an individual believes that someone else is accessing their account, they must report this immediately to the ICT Services team immediately.

8. PASSWORD GUIDELINES

8.1. Passwords are an important means of protecting users' privacy from unauthorized access. With minimal effort, users can increase the effort required by an unauthorized user to compromise information and/or privacy. The following points relate to password selection and use on all Leicester College ICT systems.

8.2. A password is defined as a secret series of alpha-numeric characters that allow a user to access a computer, program, file, or other ICT resource.

8.2.1. Passwords should not be shared. Users may receive phone calls with people claiming to be Leicester College IT employees asking for a user's password. Users should never give their password to anyone under any circumstances. Users are responsible for all activity on their account.
8.2.2. Users should log out of or otherwise lock computers or other resources when finished using them.
8.2.3. Passwords should be at least 10 characters long and contain at least one non-letter (a-z, A-Z) character. Passwords should not be the same as users' login ID and should not be a word found in a dictionary.
8.2.4. Passwords should not be written down and left in insecure locations. Insecure locations include, but are not limited to, under the system keyboard, system monitor or desk.
8.2.5. The system will automatically ask you to change your password(s) regularly.
8.2.6. Most incidents of computer "hacking" or other forms of uninvited intrusions are the result of poor password selection or protection. The College ICTS personnel may occasionally audit passwords as part of a security exercise. If a password is found that does not meet requirements for complexity and length, the user will be notified and asked to change their password to meet the requirements.

9. DEVICE/LAPTOP SECURITY GUIDELINES

9.1. This section provides recommendations where laptop computers and other mobile devices are used. The Policy is equally applicable to contractors, service providers and other organisations or agencies that use laptop computers to process Leicester College information in the performance of their duties.

9.2. Introduction

9.2.1. Mobile devices taken outside secure Leicester College environments are subject to special security risks, they may be lost or stolen and may be exposed to unauthorised access or tampering. Devices taken abroad may also be at risk, for example confiscated by police or customs officials.

9.2.2. Device loss will mean not only the loss of availability of the device and its data but may also lead to the disclosure of sensitive information, such as student assessment data. This loss of confidentiality, and potential integrity, will often be considered more serious than the loss of the physical asset and may put the College in breach of the Data Protection Act.

9.2.3. Where data should not be stored on the device but on the cloud and/or network storage systems provided.

9.2.4. If quantities of Leicester College data are held on a single device (or any other storage medium) risk assessments must consider the impacts of loss of all data. Note that deleted files should be assumed to persist on the device's hard disk.

9.3. Key Points

9.3.1. Traditional password protection of a device offers limited defence against a determined attacker because the attacker has unconstrained access to the physical device. Modern complex password techniques offer more protection which must therefore be used.

9.3.2. The physical security controls that are possible within the Leicester College buildings environment are not available outside of that environment; therefore, if procedural and personal controls of the device are breached the only effective technical measure that can be applied is encryption.

9.3.3. Unauthorised access and tampering with a device, particularly if there are repeated opportunities for access, may:

- Lead to continuing (and undetected) compromise of information on the device itself.
- Undermine security measures (including encryption); intended to protect information on the device in the event of loss or theft; and
- Lead to compromise systems to which the device is connected, for example, a networked system that is accessed from the laptop.
- The impact of a breach of device security may therefore extend far more widely than the device itself.

9.4. Security of Equipment Off-Premises

9.4.1. Security should be applied to off-site equipment considering the different risks of working outside the organisation's premises.

9.4.2. Security risks, e.g., of damage, theft, or eavesdropping, may vary between locations and should be considered in determining the most appropriate controls.

9.5. Mobile Devices and Communications

9.5.1. The appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.
9.5.2. Exceptional care should be taken to ensure that business information is not compromised. Users should take care and make themselves aware of the risks of working with mobile computing equipment in unprotected environments.
9.5.3. If lost or stolen the user must call ICT Services immediately on 01162242250 or e-mail 121@leicestercollege.ac.uk. ICT Services will decide to block the device. Any loss of equipment containing personal data must also be reported immediately to the data protection officer dpo@leicestercollege.ac.uk.
9.5.4. If damaged the user must return it to ICT Services who will arrange for the issue of a standard replacement device (not a premium or optional handset). It is up to the user's line manager to decide whether the user will have to financially contribute towards the cost of the replacement device.
9.5.5. The equipment must be returned in the condition received to ICT Services when the employee terminates employment for any reason.
9.5.6. Although College equipment is insured whilst in the College and in the course of College business, it may not be insured whilst not in use or on College sites and therefore users must be aware that their department will need to pay for replacement if lost, damaged or stolen. It is at the department manager's discretion whether to ask for a contribution from the staff user towards the replacement of the equipment.
9.5.7. Leicester College reserves the right to recharge the individual concerned if high usage/costs are deemed unnecessary or not work related.
9.5.8. International travel is sometimes required for work purposes. Where this is required, the employee should e-mail their mobile number and destination to 121@leicestercollege.ac.uk and/or call 0116 2242250 before leaving the Country. This will ensure that appropriate tariff is selected. Personal use of mobile phones abroad is not allowed, and any charges incurred due to personal use will be recharged to the employee.
9.5.9. Staff are required to abide by the current legislation when using the device whilst driving. Leicester College takes no responsibility whatsoever for the consequences of unlawful behaviour or any other malpractice.
9.5.10. Staff found to be in breach of this Policy may be subject to disciplinary action and/or legal action if a criminal offence has been committed.
9.5.11. Leicester College will review this Policy from time to time or at the point of contract renewal with the mobile phone provider.

9.6. Security Measures

9.6.1. Ensure that device(s) are not left unattended when working off-site.
9.6.2. When travelling and not in use, ensure that device(s) are stored securely out of sight. For example, when travelling by car, ensure laptops are locked in the boot. Devices left on display and unattended will inevitably attract attention and are likely to be stolen.

9.6.3. It is good practice to carry laptops in protective anonymous bags or cases (i.e., those without manufacturer logos on them) when not in use.

9.7. Other Good Practice Security Measures

9.7.1. Do not leave laptops or mobile devices unattended in car boots overnight.

9.7.2. Do not leave device(s) unattended in insecure areas, for example meeting rooms next to areas of public access, and hotel rooms where others may have access. Make use of room locks and lockable storage facilities where available.

9.7.3. Be aware of the potential for opportunist or targeted theft of laptop bags in busy public places including airports, train stations, hotel lobbies, exhibition halls, etc, and on public transport e.g., buses and trains.

9.7.4. When travelling avoid placing devices in locations where they could be easily forgotten or left behind e.g., overhead racks and taxi boots.

9.7.5. Be aware that the use of laptops in public places will draw the attention of those in the vicinity. It is possible that information viewed on a laptop screen could lead to the unauthorised disclosure of that information being processed.

10. RECORDING AND TRANSCRIPTION

10.1. The Office 365 suite includes tools which enable the recording of images/video/audio and the transcription of the spoken word. We recognise that these may be useful tools for both students and staff.

10.2. Students wishing to use recording or transcription tools should seek written consent in advance of the session from the relevant lecturer/tutor; where consent is refused, the recording should not take place. Consent is not required for transcriptions where the use of transcription is set out in an EHCP or has been identified as a reasonable adjustment by the College. Further information is set out in the Recording Lectures and Demonstrations Policy (HR043).

10.3. Staff wishing to use recording or transcription tools should follow the procedure set out in section 5 of the Recording Lectures and Demonstrations Policy (HR043).

10.4. The College may make any recordings and transcriptions and make these available to students for personal use only. They remain the property of the College and should not be reproduced without written permission. Appropriate copyright statements will be included in any recordings. Lecturers will be correctly identified in any transcription. In line with the contract of employment, copyright in the recording or transcription will be owned by the College.

11. LEGAL CONSTRAINTS

11.1. Software may not be copied, installed, or used on the Leicester College IT equipment except when and as permitted by the owner of the software and by law and with agreement from Leicester College ICT Services. The department will properly license software and strictly adhere to all licensing provisions,

including installation, use, copying, number of simultaneous users, and terms of the licence.

11.2. It is up to the user to check the terms and conditions of any licence for the use of the software or information and to abide by them. Software provided by Leicester College ICT Services may only be used as part of the user's duties as an employee or student or for educational purposes.

11.3. The user must abide by all the licensing agreements for software entered by Leicester College with other parties, noting that the right to use any such software outside Leicester College premises will cease when an individual leaves the institution. Any software on a privately owned computer that has been licensed under a Leicester College agreement must then be removed from it, as well as any Leicester College owned data.

11.4. The user must comply with all the relevant legislation and legal precedent, including the provisions of the following Acts of Parliament, or any re-enactment thereof:

- Copyright, Designs and Patents Act 1988
- Malicious Communications Act 1988
- Computer Misuse Act 1990
- Criminal Justice and Public Order Act 1994
- Trademarks Act 1994
- Data Protection Act 2018
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Communications Act 2003
- Criminal Justice and Immigration Act 2008.

11.5. Any breach of the above legislation or related policies is an offence and in that event Leicester College disciplinary procedures will apply. Appendix 1 provides more detail. For further information, please contact ICT Services via 121@leicestercollege.ac.uk or call 0116 2242250.

12. ACCESSIBILITY

12.1. Leicester College is committed to ensuring digital accessibility for people with disabilities. We are continually improving the user experience for everyone and applying the relevant accessibility standards.

12.2. Measures to support accessibility:

- Integrate accessibility into our procurement practices
- Provide continual accessibility training for our staff
- Include people with disabilities in our design personas.

12.3. We realise that for a variety of reasons - technical, sensory, or cognitive - disabled students and staff can take longer to navigate to resources and may

need to personalise them to use them effectively. As a result, the College will provide access to technologies such as eBook readers, browser plugins to read content aloud, Learning Tools plugin in Microsoft Office products including specialised hardware to aid teaching and learning activities.

12.4. The College's accessibility statement can be found at https://leicestercollege.ac.uk/about/accessibility-statement/

13. COMMUNICATION AND REVIEW

13.1. This Policy will be communicated as part of the relevant induction process.

13.2. The Policy will be reviewed at least every three years by the Executive Leadership Team.

APPENDIX

Legal constraints - references

Copyright, Designs and Patents Act 1988

This Act, together with several Statutory Instruments that have amended and extended it, controls copyright law. It makes it an offence to copy all, or a substantial part, which can be a quite small portion, of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy lesser amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, sound, moving images, TV broadcasts and many other media.

Malicious Communications Act 1988

Under this Act it is an offence to send an indecent, offensive, or threatening letter, electronic communication, or another article to another person. Additionally, under the Telecommunications Act 1984 it is a similar offence to send a telephone message, which is indecent, offensive, or threatening.

Computer Misuse Act 1990

This Act makes it an offence:

- to erase or amend data or programs without authority
- to obtain unauthorised access to a computer
- to "eavesdrop" on a computer
- making unauthorised use of computer time or facilities
- maliciously to corrupt or erase data or programs
- to deny access to authorised users

Criminal Justice and Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm, or distress, they:

- use threatening, abusive or insulting words or behavior, or disorderly behavior; or
- display any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm, or distress.

Trademarks Act 1994

This Act provides protection for Registered Trademarks, which can be any symbol (words or images) or even shapes of objects that are associated with a particular set of goods or services. Anyone who uses a Registered Trademark without permission can expose themselves to litigation. This can also arise from the use of a Mark that is confusingly like an existing Mark.

Data Protection Act 2018
This sets out the rights and responsibilities of individuals and those processing any personal data. The College's Data Protection Policy provides more detail. This sets out the rationale and processes for governing the processing of personal data, the use of privacy notices, the responsibilities of staff and students, principles around data security and individuals' rights to their data.

Everyone has rights about how their personal information is handled. During our activities we will collect, store and process personal information about our students, staff, employers, visitors and members of the public and we recognise the need to treat it in an appropriate and lawful manner.

The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Act and other regulations. The regulation imposes restrictions on how we may use and how we store and safeguard that information.

Human Rights Act 1998
This act does not set out to deal with any mischief or address specifically any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the context of the College, important human rights to be aware of include:

- the right to a fair trial
- the right to respect private and family life, home, and correspondence
- Freedom of thought, conscience, and religion
- freedom of expression
- freedom of assembly
- prohibition of discrimination
- the right to education

These rights are not absolute. The College, together with all users of its ICT services, is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations which arise from other relevant legislation.

Regulation of Investigatory Powers Act 2000
The Act states that it is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic (including telephone) communications is permitted to:

- Establish the facts
- Ascertain compliance with regulatory or self-regulatory practices or procedures
- Demonstrate standards which are or ought to be achieved by people using the system
- Investigate or detect unauthorised use of the communications system
- Prevent or detect crime or in the interests of national security
- Ensure the effective operation of the system

Freedom of Information Act 2000
The Act, intended to increase openness and transparency, obliges public bodies, including Educational Institutions, to disclose a wide range of information, both

proactively and in response to requests from the public. The types of information that may have to be found and released are wide-ranging, for example minutes recorded at a board meeting of the institution or documentation relating to important resolutions passed. Retrieval of such a range of information places a considerable burden on an institution subject to such an information request. In addition to setting a new standard of how such bodies disseminate information relating to internal affairs, the Act sets time limits by which the information requested must be made available, and confers clearly stated rights on the public, regarding such information retrieval. Therefore, all staff have a responsibility to know what information they hold and where and how to locate it.

Communications Act 2003
This act makes it illegal to dishonestly obtain electronic communication services, such as e-mail and the World Wide Web.

Criminal Justice and Immigration Act 2008
This act increased the penalties for publishing an obscene article. It also introduced fines for data protection contraventions when organisations 'knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial distress or damage but failed to take reasonable steps to prevent the contravention.'