Information Technology Usage & Data Handling Policy

2021 - 2023

Policy Owner	Vice Principal: Corporate Services
Policy Status	Final
Policy Version	V5
Approved By	College Management Team (CMT)
Approval Date	June 2021
Review Date	June 2023
Distribution	All

Contents

1. Introduction

Burton and South Derbyshire College seeks to promote and facilitate the responsible and extensive use of Information Technology in the interests of learning, research and ongoing College business. Burton and South Derbyshire College is committed to the protection and safeguarding of its learners whilst using such systems. This policy is intended to provide a framework for such use and applies to all computing, telecommunication and networking facilities provided by any department or section of the College. The items in the policy are not recommendations or guidelines. Contravention of the policy may lead to disciplinary action being taken against the individual/s.

2. Authorisation and Acceptance

Usage of the College's IT services is conditional upon the acceptance of this policy for which a signature of acceptance will be required before joining the college. For staff this is via acceptance of an employment contract and/or completion of a Staff ID request form, and for students by the completion of an enrolment form. Failure to provide a signature for this policy will not exempt an individual from any obligations under this policy.

Policy acceptance grants the individual authorisation to use the College's IT facilities. If the policy is not accepted then an individual will not have the right to a computer user logon account which might have a serious repercussion on the individual's employment or course progression.

Following employment commencement or enrolment a username, password, file storage area and e-mail address will be allocated for the individual to utilise during their course or employment period at the College.

3. Monitoring and filtering

Burton and South Derbyshire College will maintain appropriate monitoring arrangements in relation to all IT services and facilities that it provides, and the College will apply these monitoring arrangements to all users.

These arrangements may include logging, checking and/or filtering content, and in some instances recording activity for the purpose of:

- Establishing the existence of facts relevant to the business.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of IT facilities and systems.
- Ensuring effective operation of IT facilities and systems.
- Ensuring compliance with this policy.
- Determining if communications are relevant to the business (for example where an employee is off sick or on holiday and written authorisation from a senior manager has been received.)

The College may, at its discretion, apply additional logging, checking and/or filtering as appropriate, and deny the transmission and/or receipt of certain data which might be deemed unacceptable under the terms of this policy. These monitoring arrangements may operate on a continual or ad hoc basis as required in order to ascertain policy compliance.

3.1. College Prevent policy

Prevent aims to stop people becoming terrorists or supporting terrorism. Education, like other key sectors, has a responsibility to promote values of openness, tolerance and facilitating free debate which is central to being a British Citizen. With the current government alert at severe (2017) the College needs to be aware of risks and raise awareness within its community

To help enforce the Prevent strategy within the College the following it measures have been incorporated

- All known extremist sites and content relating to Prevent will be blocked for all staff and students using regularly updated databases.
- The college firewall checks for key words within searches and will block at a high level to prevent further use and logged within the current IT systems.
- A weekly report is sent to the "Director of IT and Estates" highlighting any persons found to be searching for identified keywords relating to the prevent policy, this list is then forwarded to the "Deputy Principle Corporate Relations" for action.
- A full copy of the Prevent strategy can be found on the college intranet policies section.

4. Email

Access and usage of the College email service is permitted for legitimate business purposes. Limited personal usage is accepted providing that this in no way restricts or impairs normal College business operations or system availability/resources, is in line with current Safeguarding policies and is not of a commercial or profit-making nature unless connected with a legitimate College venture via authorisation from a senior member of staff.

Due to the implementation of a central email filtering system aimed at protecting the College network from security concerns and junk emails, some emails may be prevented from entering the college mail server. If you suspect that a mail has been blocked which you have a legitimate reason for accessing, please contact the college Helpdesk.

Burton and South Derbyshire College reserves the right to append any message or disclaimer to any/all email messages that are sent to external addresses from the College mail system.

Access to e-mail files will not be given to an unauthorised staff member unless approved by the Network and IT Manager (or suitable nominee) who will use their discretion, in consultation with other senior College members. In such circumstances the Head of Department or more senior line manager will be informed, and will normally be consulted prior to action being taken. Such access will normally only be granted in the following circumstances:

- Where a breach of the law or a serious breach of this or another College policy is suspected.
- When a documented and lawful request from a law enforcement agency such as the police or security services has been received.
- On written request from the relevant Head of Department (or more senior manager) where the managers or co-workers of the individual require access to e-mail messages or files in order to continue normal College business and the individual is unable to provide them.

4.1. Acceptable Usage

Use of the College email system by staff and students is permitted and encouraged where such use supports the goals and objectives of the business and its learners. In accessing and using the College email system staff and students must ensure that they:

1. Check their email daily during the working day.
2. Send emails to the correct recipients.

3. Are vigilant when sending sensitive or private emails to mailing groups.
4. Employ good house-keeping practices by ensuring emails which are no longer required are permanently deleted.
5. Encrypt file attachments sent (outside of the organisations email system) which contain personally identifiable data.
6. Limit personal usage to an acceptable level.

4.2. Unacceptable Use

The following is deemed unacceptable use or behaviour by College staff and students:

1. The creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
2. The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
3. The creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
4. The creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
5. The creation or transmission of defamatory material.
6. The creation or transmission of material that is illegal.
7. The creation or transmission of material that includes false claims of a deceptive nature.
8. Unreasonable or excessive personal use.
9. Activities that corrupt or destroy other users data or disrupt the work of other users.
10. Undertaking activities that violate the privacy of other users.
11. Publishing to others the text of messages written on a one-to-one basis, without prior consent of the author.
12. The creation or transmission of anonymous messages, i.e. without clear identification of the sender.
13. The creation or transmission of material which brings the College into disrepute.
14. Auto forwarding emails from individuals College email accounts to personal mail accounts or vice versa. Emails are accessible via the Outlook Web Access service when outside the College.
15. Opening an attachment received via unsolicited email where it is clearly unrelated to work or study, which leads to widespread virus infection or other serious security breaches.
16. Passing on of electronic chain mail.
17. The use of College mailing lists for non-academic purposes unless authorised to do so.
18. Personally sensitive material should not be transmitted externally through an electronic messaging system unless the data is first encrypted and then added as an attachment. Do not place personal data directly into an email, always add as an encrypted attachment. This does not apply to internal emails from and to individuals whose email address ends with @bsdc.ac.uk.
19. Where personal data is being sent within the Burton and South Derbyshire College electronic messaging system via an email distribution group, care should be taken that the group contains the correct individuals to prevent unauthorised viewing.
20. Staff should not auto-forward emails from their Burton and South Derbyshire College email account to a third party email system.

5. Internet Access and Usage

Access to Internet services is permitted for legitimate business purposes. Limited personal usage is accepted providing that this in no way restricts or impairs normal College business operations or system availability/resources, is in line with current Safeguarding policies and is not of a commercial or profit-making nature unless connected with a legitimate College venture via authorisation from a senior member of staff.

Internet transactions are logged for system maintenance and performance reasons and may be seen by IT technical staff in the course of their duty. Inappropriate Internet access which is identified will be reported and progressed via the disciplinary procedures.

Access to certain Internet content via the College network may not be possible due to the implemented filtering system which attempts to protect young and vulnerable learners from harmful material and ensure an acceptable level of network availability for all staff and students. This filtering is not intended to disrupt access to content which may be required in order to undertake research for legitimate purposes. If you feel this to be the case please speak to your course tutor or senior manager who will escalate this to the college Helpdesk for review.

5.1. Acceptable Usage

Use of the Internet by College staff and students is permitted and encouraged where such use supports the goals and objectives of the business and its learners. In accessing the Internet staff and students must ensure that they:

1. Comply with current legislation.
2. Use the Internet in a responsible manner.
3. Do not create unnecessary business risk to the College by the misuse of the Internet and the associated networking resources.
4. Only use cloud storage / online systems that have their data located within the European Union and fully comply with data protection law when using identifiable or sensitive information.

5.2. Unacceptable Use

The following is deemed unacceptable use or behaviour by College staff and students:

1. Visiting Internet sites that contain pornographic material.
2. Using the Internet to send offensive, defamatory or harassing material to other users.
3. Using the internet to perpetrate any form of fraud, software, and video or music piracy.
4. Downloading of unauthorised software.
5. The downloading, uploading or distribution of music, video, film, software or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder.
6. Hacking into unauthorised areas which have not been specifically allocated to the individual.
7. Undertaking deliberate activities that waste staff effort or networked resources.
8. The deliberate or negligent introduction of any form of computer virus or other security related exploit into any College IT system or network.
9. Using messaging services, chat rooms, social networking sites or blogs in any manner that could appear to third parties to be providing an opinion or expressing a negative impression that could be attributed to Burton and South Derbyshire College or a member of Burton and South Derbyshire College staff or students, except where it has been appropriately authorised.

6. Computer Usage

Access and usage of the College computer and networking services is permitted for legitimate business purposes. Limited personal usage is accepted providing that this in no way restricts or impairs normal College business operations or system availability/resources, is in line with current Safeguarding policies and is not of a commercial or profit-making nature unless connected with a legitimate College venture via authorisation from a senior member of staff.

Remote VDI sessions connecting to college systems must be done so in a secure environment taking care to make sure they are restricted to authorized college staff/student use and at no point left unattended without appropriate security measures being implemented such as locking the session or applying a screen lock method to the device. Any information contained within the VDI sessions where any personal

data is stored should under no circumstance be saved to the local drive(s) of the current device or any systems put in place to automatically replicate data to the local drive(s)
All software contained within the college VDI environment is for the purpose of teaching and learning and should only be used as such.

All allocated usernames, passwords and e-mail addresses are for the exclusive use of the individual to whom they are assigned and will not be shared with any other individual/s. The individual is personally responsible and accountable for all activities carried out under their username and will not allow any other individual to use their account. The password associated with a particular username must not be divulged to any other person, other than to designated members of IT staff for the purposes of system support. Attempts to access or use any username, e-mail address or file storage area which has not been specifically allocated to the individual may result in disciplinary action. All users must correctly identify themselves at all times and must not attempt to falsify, withhold or tamper with their information in order to appear as another user.

A user must take all reasonable precautions to protect their resources by ensuring their password adheres to acceptable standards. This advice must be followed and failure to do so may be regarded as a breach of this policy. If in doubt, please contact the IT Helpdesk.

IT equipment which is not owned and supported by Burton and South Derbyshire College should not be attached to the wired network without the prior consent of the IT Department. Attempts to do so may result in the spread of viruses or malicious code which will be deemed as a breach of this policy. Where wireless networking technology is available within flexible working spaces, security prevention technology will be enforced automatically.

6.1. Unacceptable Use

The following is deemed unacceptable use or behaviour by College staff and students:

1. The retention or distribution of material that is offensive, obscene or indecent.
2. Intellectual property rights infringement, including copyright, trademark, patent and design.
3. Causing annoyance, inconvenience or needless anxiety to others through the use of College IT services and systems.
4. Attempts to break into or damage computer systems or data held thereon.
5. Actions which intentionally or unintentionally aid the distribution of computer viruses or other malicious software.
6. Actions intended to facilitate access to computers for which the individual is not authorised.
7. Using the College network for unauthenticated access.
8. Unauthorised resale of College equipment, services or information.
9. The distribution or storage of music, video, film, software or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder.
10. The publication on external websites of unauthorised recordings, e.g. of lectures.
11. Monitoring or interception of network traffic, without permission.
12. Probing for security weaknesses of systems without permission.
13. Associating any device to network Access Points, including wireless, for which you are not authorised.
14. Non-academic activities which generate heavy network traffic, especially those which interfere with legitimate use of IT services or systems by other individuals.
15. Excessive use of system resources such as file storage areas, leading to a negative impact on others, especially when the issue has already been brought to an individual/s attention for remedial action.
16. Frivolous and irresponsible use of College owned computers where such activities interfere with the legitimate use of IT services by others.
17. The deliberate viewing and/or printing of pornographic images.

18. Installing and or running of software which has not been approved by the IT Department.
19. The creation of web based content, portraying official College business without express permission.
20. The use of CDs, DVDs, USB drives and other storage devices for copying software and material that is unlicensed, copyrighted or not licensed to the college.
21. The copying of other people's web site, or other, material without the express permission of the copyright holder;
22. The use of peer-to-peer networking solutions and related applications within the College.
23. The intentional use of other people's material without their consent.
24. Using an unencrypted mobile device to hold and transport personally identifiable or sensitive data.
25. Deliberately attempt to circumvent or disable implemented security systems which might otherwise place data at risk of exposure to unauthorised individuals.
26. Saving personally identifiable or sensitive data to the local hard drive of a College owned desktop or mobile computing device without the presence of a data encryption solution.
27. Leaving workstations logged in and unlocked whilst unattended.
28. Intentionally jeopardising the integrity, performance or reliability of College computer equipment, software, data and other stored information.
29. Interfering or attempting to interfere with information belonging to or material prepared by another individual without the express permission of the owner.
30. Making unauthorised copies of information belonging to another user without the express permission of the owner.
31. The use of any software not installed onto the computers by the IT department unless specifically authorised by an appropriate lecturer or manager.
32. Staff should not deliberately attempt to circumvent or disable implemented security systems which might otherwise place data at risk of exposure to unauthorised individuals. *
33. Staff are responsible for ensuring their individual passwords are kept safe. They will not be shared, copied, written down, opening discussed or easily-guessed. Extra care should be taken in public and communal areas when typing usernames and passwords

* Without the express authorisation from IT Departmental Management

7. Telephony

Desktop telephone handsets, mobile telephones, smart phones and data devices which employ mobile telephony technologies (such as 3G) are provided by the College for legitimate business and/or health and safety requirements (such as lone working). Limited personal usage is accepted providing that this in no way restricts or impairs normal College business operations or College system availability/resources, is in line with current Safeguarding policies and is not of a commercial or profit-making nature unless connected with a legitimate College venture via authorisation from a senior member of staff. Where there is evidence of a high level of personal usage which is not compliant with this Policy, the individual responsible will be liable to pay any excess call charges and may be subject to disciplinary procedures.

International dialling and premium rate services may by restricted. Where this is the case, the restriction may be lifted following a request to the IT Helpdesk from the individual’s senior manager.

7.1. Acceptable Usage

Whilst using college allocated telephone services staff and students (where appropriate) will ensure that:

1. A professional and courteous manner is employed whilst using college based telephony services.
2. College allocated phones which employ voice mail are pin protected and that the pin is changed to something unique.
3. College allocated phones which employ voice mail is checked daily whilst in the office.

4. College allocated smart phones and data devices which are capable of receiving College email must be protected by a pin or password.
5. Mobile phones and data devices are to be used in a safe manner and in accordance with Health and Safety advice.
6. Appropriate basic security measures are employed to help minimise loss or theft of a mobile phone or data device both inside and outside the college.
7. Any form of digital communication from a college allocated telephony or data device is kept professional and does not contain sensitive information. In the case of email messages, please refer to the appropriate section of this policy.
8. Report the loss or theft of a college allocated mobile phone or data device immediately to the IT helpdesk.
9. Care is taken when dialling telephone numbers in order to minimise costs relating to premium rate, international and mobile-to-mobile calls. Wherever possible, calls should be made to landline numbers in the first instance.

7.2. Unacceptable Use

The following is deemed unacceptable use or behaviour by College staff and students:

1. Sending or transmitting a telephone conversation which is deemed indecent, offensive, or threatening.
2. Interaction with any mobile phone or data device whilst driving for college related business. This includes the use of a hands free solution in line with the College Driving for Work policy.
3. Not returning college allocated mobile phones or data device once the individual has left the employment of the college.
4. Using a personally owned Smartphone or other such data device which is configured with College email account settings, without the employment of a suitable security measure such as a pin or pass code.
5. Deliberately deactivating or removing implemented security measures on a College allocated Smartphone or other such data device.

8. College Copyright Material

Any software, data and/or paper-based information which is not generated by the individual and which may be available through the use of the College computing or communications resources shall not be copied or used without permission of the College or the copyright owner. It is up to the individual to check the terms and conditions of any licence for the use of this data or information and to abide by them. Software, data and/or paper-based information provided by the College may only be used as part of the user's duties as an employee or student of the College or for educational purposes.

The user must abide by all the licensing agreements for software entered into by the College. Any software or College owned-data on a privately owned computer that has been licensed under a College agreement must be removed immediately by the individual once they leave the employment of the college or when their course has concluded.

In the case of private work and other personal data which is contained on College equipment, the College will not accept any liability for loss, damage, injury or expense that may result.

9. Disciplinary action

In circumstances where there is a report or suspicion relating to a potential breach of this policy the College will, as a first action, act promptly to prevent continuance or repetition of the breach, for example to withdraw any unacceptable material or to prevent further exposure to potential security breaches. This action will be taken in accordance with the normal managerial arrangements, and will typically involve liaison between The IT Department and the appropriate member/s of the College Management Team.

Subsequent action will be as described below.

- Indications of non-compliance with this policy will be investigated in accordance with the provisions of the College disciplinary procedures as applicable to staff and students. This may involve the reviewing of log files and/or email and file content where stored on or in College IT systems.
- Subject to the findings of any such investigation, non-compliance with this policy will lead to appropriate disciplinary action which could include suspension or dismissal.
- In such cases where of a criminal offence may be suspected, the issue will be reported to the police for them to take appropriate action.

The College reserves the right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and / or other contraventions of this policy.

10. PERSONAL DATA HANDLING AND SECURITY

It is the responsibility of all College staff members to ensure that the handling, transportation, disposal and storage of personal data and documentation are done responsibly and lawfully. Personal information is precious, so it should be treated in the same way you would any other valuable item. In order to protect and safeguard our students, business partners and staff members it is critical that the specifics of this policy are adhered to at all times whether it is for computer or paper based systems.

Personal data is classified as any information which directly or indirectly helps to identify a living individual. This might include any single or combination of the following:

- Name
- Address
- Email address
- Telephone number
- Ethnicity
- Date of birth
- National insurance number
- Bank details
- Training records
- Enrolment details
- Passport number
- Place of employment
- Place of study
- Student/Staff Identification
- Academic performance details

It is important to note that a name alone may not be enough to identify an individual. An example would be John Smith where several people may have the same name. However, if this name is combined with a place of study or address this could then be classed as personal data. A combination of different information such as gender, ethnicity and work location may very well enable you to identify a particular person from a larger group

<u>Protection of computer based personal data</u>

It is important that individuals review the type of information they handle within their working environment to help identify what is classed as personal data in relation to this policy. Once this is done, the following points need to be adhered to:

- Staff members should save all files containing personal data to the network server (for example the S: drive for shared data) to ensure its security.
- Personal data should be held within a secure folder on the network server which has restricted access applied.
- All allocated computers, laptops, personal digital assistants (PDA) and phones should be secured with a password or pin.
- ID cards and other access devices should be held securely on one's person or within a locked draw or cabinet when not in use.
- All mobile computing devices (i.e. laptops, tablets, Personal Digital Assistants (PDAs), USB flash drives, and handheld devices) should be physically secured within a locked draw or cupboard when not in use and must be password protected.
- Staff should be vigilant about the positioning of computer screens to prevent unauthorised individuals from viewing personal data. Please raise any concerns with your line manager.
- Access to areas which contain personal data should be restricted with door locks, key pads or swipe cards and secured when not in use.

Transport and transmission of computer based personal data

Consideration needs to be given when personal data is moved outside of the secure College environment and into an uncontrolled area. The easiest way to prevent the loss or theft of this data is to utilise centrally provided solutions which avoid the need for this external movement. However, if it is deemed essential for this data to be transported or transmitted then the following points need to be adhered to:

- Personal data should not be taken off-site unless authorised to do so by your program area manager or department manager.
- Personal data should not be transmitted via a wireless network connection to or from a portable computing device unless an encrypted wireless transmission protocol is used. Within the college this connection will provided and secured by the IT department.
- If you transmit personal data over a home wireless connection you must have the WPA protocol configured as a minimum security level. Ask your home network supplier for additional information.
- Users of mobile computing devices should be extra vigilante whilst transporting devices which contain personal data to prevent loss, theft or damage.
- Lost or stolen computing devices which may contain personal data should be reported as soon as possible to the IT Helpdesk (Ext: 4444, email: helpdesk@bsdc.ac.uk).

Securing paper based data

Personal data held on and within paper based systems needs to be controlled in order for details to remain safe during processing, storage and transportation. Please review the content of such systems within your area and ensure the following points are adhered to:

- Paper based personal data should not be taken off-site unless authorised to do so by your program area manager or department manager.
- Paper based personal data should never be left unattended by the authorised user in a vehicle during or after transportation.
- When not in use, paper documents containing personal data should be locked in a draw or cupboard even if security measures have been implemented on external store, office or classroom doors.
- Documents shall be disposed of in a safe and secure manner. Use confidential waste bags or shredding for documents containing personal data.
- If documents which contain personal data need to be printed or photocopied, these should be picked-up immediately after the job has been submitted and carefully filed appropriately.
- If using the College internal postage system for the sending of paper based personnel data you must ensure it is securely sealed into an envelope marked 'Private and Confidential' and clearly labelled with the intended recipients name and department.

- If paper based personal data is being sent externally via a third party postal service, you must ensure that it is sent either by a secure courier company or via recorded delivery and proof of postage is kept in a safe place.

Reporting suspected violations and concerns

Staff shall report security related events; known or suspected violations; and inappropriate, unethical, and illegal activities relating to the secure handling, storage, disposal or transferal of personal information. Staff shall contact the Data Security Officer at datasecurity@bsdc.ac.uk

What support is available?

If you handle personal information which is held in electronic form and require this to be transported off or between sites, please contact the IT Help Desk on Ext: 4444, email: helpdesk@bsdc.ac.uk

Confidential waste bags can be ordered via reprographics. When full please call Property Services for collection on Ext: 4531, email: estates@bsdc.ac.uk

If you hold personal information in a paper based system and require lockable storage please contact Ext: 4553, email: securestorage@bsdc.ac.uk.

If you require any advice on data security, handling or have a general enquiry in relation to this policy please contact the Data Security Officer at datasecurity@bsdc.ac.uk

11. Policy Supervision and Advice

The IT Department is responsible for the supervision of this policy. A senior member of the IT Department will be designated as the person responsible for the ongoing management of the policy's enforcement. They will liaise with the Network and IT Manager and any other appropriate senior member as and when required. Procedural guidelines will be published from time to time as a separate document when required.

This policy is not exhaustive and as new social and technical developments occur this will lead to further updates to this policy. In the first instance students should address questions concerning what is acceptable to their course tutor or supervisor. Staff should initially contact their Program Area Manager or Departmental Manager.

12. Legal Requirements

Individuals must comply with all relevant legislation including the following Acts of Parliament:

Copyright, Designs and Patents Act 1988 www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

Malicious Communications Act 1988 www.opsi.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm

Computer Misuse Act 1990
www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Criminal Justice and Public Order Act 1994
www.opsi.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm

General Data Protection Regulation (GDPR)
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Regulation of Investigatory Powers Act 2000 www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
www.opsi.gov.uk/si/si2000/20002699.htm

Communications Act 2003
www.opsi.gov.uk/acts/acts2003/ukpga_20030021_en_1

Criminal Justice and Immigration Act 2008
www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_1

See below for a summary of the main points. Further advice should be obtained through the Head of IT in the first instance.

12.1. Copyright, Designs and Patents Act 1988

This Act controls copyright law. It makes it an offence to copy all, or part of copyright protected work or material. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small 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.

12.2. Malicious Communications Act 1988

Under this Act it is an offence to send an indecent, offensive, or threatening letter, electronic communication or other 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.

12.3. 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.
- To make unauthorised use of computer time or facilities.
- To maliciously corrupt or erase data or programs.
- To deny access to authorised users.

12.4. Criminal Justice & 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 behaviour, or disorderly behaviour; 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.

12.5. Data Protection act 2018 / General Data Protection Regulation

Burton and South Derbyshire is committed to a policy of protecting the rights and privacy of individuals (includes students, staff and others) in accordance with the Data Protection Act. The College needs to process certain information about its staff, students and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The policy applies to all staff and students of the College. Any breach of the General Data Protection Regulation, Burton and South Derbyshire Data Protection Policy or Burton and South Derbyshire Data Security Policy is considered to be an offence and in that event, disciplinary procedures will apply.

12.6. Regulation of Investigatory Powers Act 2000

This Act permits organisations to monitor telephone calls, faxes and emails with the consent of the employees and the express or implied consent of external parties concerned in the communications being monitored.

12.7. Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This Act permits the employer to monitor and/or keep a record of any form of electronic (including telephone) communications, in order to:

- Establish the facts.
- Ascertain compliance with regulatory or self-regulatory practices or procedures.
- Demonstrate standards, which are or ought to be achieved by persons 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.

Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal.
- Protect or support help line staff.

Burton and South Derbyshire reserves the right to monitor e-mail, telephone, and any other communications in line with its rights under this act.

12.8. Communications Act 2003

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

12.9. 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.’