Information Technology Conditions of Use

Author	Director of IT
Date	May 2023
Person Responsible	Director of IT
Approval/review body	SLT and DPO
Frequency of Review*	24 months

** Policies will be reviewed more frequently if legal changes or good practice require*

Review History:		
Date of review	**Reviewed by**	**Reason for review**
June 2012	Executive Director of IT	General update to include staff and students via Student IT User Guide
October 2015	Executive Director of Facilities and resources	Re-write to include changes regarding cloud and mobile data
December 2016	Executive Director of Facilities and resources	Minor changes to policy regarding USB data storage
August 2018	Executive Director of Facilities and resources	Review and make changes to accommodate UK and EU data protection changes
September 2019	Executive Director of Facilities and resources	Add references to reference the student IT Guide as the reference guide for IT Policy for students
November 2021	Director of IT	Changes relating to private devices; use of home IT; instant messaging and Cyber Security
May 2023	Director of IT	Minor change to cover sharing of explicit material

Contents

Related policies and Procedures:

1. Dealing with Malicious Communication Procedure
2. Data Breach Policy and Procedure
3. Mobile Device and Communication Policy
4. Data Protection Policy and Procedure
5. College Business Continuity Plan
6. Information Technology Business Continuity Plan
7. Staff Code of Conduct
8. Equal Opportunities Policy
9. Anti-harassment Policy
10. Staff Disciplinary Policy and Procedure

NOTE: This Policy together with the Policies and Procedures listed above, seeks to ensure, so far as reasonably practicable, that the College is fulfilling its duty under sections 26 and 29 of the Counter-Terrorism and Security Act 2015 and the Prevent Duty. The College will participate fully in work to prevent people from being radicalised or drawn into extremism and will ensure that, should this occur, there are procedures in place to deal with them.

1. Statement

These "Conditions of Use" apply to the use of all computer, electronic Information Technology ("IT") and communication facilities by all staff and students at North Kent College, which incorporates Hadlow College, ("the **College**").

2. About this policy

2.1 Our IT and communications systems are intended to promote effective communication and working practices within and with the College. It is also intended to protect the College from improper and inappropriate use of its systems and to assist with the provision and creation of a safe place of work and study.

2.2 The operation of electronic communications systems is likely to involve the processing of personal data and our activities are therefore regulated by the UK and European legislation, together with the Employment Practices Data Protection Code, issued by the Information Commissioner. The College is also required to comply with *Regulation of Investigatory Powers Act 2000*, the *Telecommunications (Lawful Business Practice) (Interception of Communications Regulations 2000 (SI 2000.2699)* and the principles of the European Convention of Human Rights incorporated into United Kingdom law by the *Human Rights Act 1998.* For information in respect of these acts and regulations see Appendix 1.

2.3 This policy sets out the standards you must observe when using the College's systems, the circumstances in which the College will monitor your use, and the action it will take in respect of breaches of this policy.

2.4 The conditions form part of staff conditions of employment and student learner agreement and may be varied from time to time. It is essential that staff read this document.

2.5 The conditions are set out and communicated to students through the "Student Digital & Learning IT Guide" which is updated annually in line with this policy and distributed to students during enrolment.

2.6 All staff and students are required to acknowledge acceptance of the potential liabilities involved in using email and the Internet by a splash screen, which will appear each time they log-on to the College system, and they will need to make their students aware as well.

2.7 Misuse of IT and communication systems can damage the College's business and reputation. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

3. Key principles

3.1 Staff are required to observe the following precepts:

3.1.1 **Integrity**

The accuracy and completeness of information within the College must be safeguarded.

3.1.2 **Confidentiality / Data Protection**

The security of data, including sensitive and/or personal information which must be protected from unauthorised access, disclosure or interception.

Personal data under UK Data Protection Act 2018 is any data information relating to an identifiable person who can be directly or indirectly identified ("in particular" by reference to an identifier) including (but not limited to), names (abbreviations should be used instead), birth dates, address information.

Special Category Data is defined as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

3.1.3 **Legality**

Material held or transmitted using the College's IT and communications system must respect copyright and conform to national and international law.

4. Equipment Security and Passwords

4.1 Staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

4.2 Staff are responsible for the security of any computer terminal used by them and for any handheld device such as mobile phone, laptop or data pad which may be given to them to perform their role. Staff should lock their terminal or log off when leaving a computer or device unattended or on leaving the office/room (even if the office/room is locked), to prevent unauthorised users accessing the system in their absence. Anyone who is not authorised to access our network should only be allowed to use terminals under our supervision.

4.3 Desktop PCs (including Macs) and cabling for telephones or other computer equipment should not be moved or tampered with without first consulting the IT Department.

4.4 The College reserves the right to retrieve a staff member's password in order to check his/her email or internet usage or files as reasonably necessary in the interests of the business, for example (but not limited to) assisting in the investigation of alleged wrongdoing, to retrieve lost messages or to comply with any legal obligation. Any request for access to a staff member's files and email must be made in writing by the Head of HR to the IT Department.

Staff members must provide their password within five working days of any written request being made by the Human Resources Department ("HR") and any password should not be unreasonably withheld. A failure to do so will be considered by the College to be a failure to follow a reasonable instruction for which disciplinary action may be taken and access to IT systems may be barred.

4.5 The College uses a data information security system where staff can encrypt files and email. The College reserves the right to unencrypt any files or email stored on College systems as necessary in the interests of the business, for example (but not limited to) assisting in the investigation of alleged wrongdoing, to retrieve lost messages or to comply with any legal obligation. Any request for access to a staff member's files and email that is encrypted must be made in writing by the Head of HR to the IT Department (IT Manager).

4.6 Staff should use strong passwords on all IT equipment, including items that are taken off the College's premises. Staff must keep passwords confidential and change them regularly (every 90 days). Staff must not use another person's username and password or make available or allow anyone else to use their username and password unless authorised by the IT Department. On the termination of employment (for any reason) staff must provide details of their passwords to the IT Department if requested and return all IT and communications equipment.

4.7 If staff have been issued with a laptop, data pad, mobile phone or data storage device, they must ensure that it is kept secure always, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft. Staff should also be aware that when using equipment away from the College, documents may be read by third parties, for example, passengers on public transport.

5. E-mail

5.1 Although e-mail is a vital business tool, staff should always consider if it is the appropriate method for a communication. Correspondence with third parties by e-mail should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

5.2 Email should not contain any personal information (meaning any information relating to an identifiable person who can be directly or indirectly identified "in particular" by reference to an identifier) as defined by UK and EU Data Protection Laws, including (but not limited to), names (abbreviations should be used instead), birth dates, address information or special data detailing medical/health, religion, sexual orientation, ethnic origin or political / trade union membership. The College provides easy to use one click classification for email and data attached that has embedded protection rules associated.

If as a part of College business, personal information (as described above) needs to be sent via email, permission needs to be obtained from the Data Protection Officer. Any such email MUST be encrypted before sending (using the provided mechanisms) or attached documents MUST be password protected (passwords may not be sent by email).

5.3 Due to the informal nature of e-mail, it is easy to forget that it is a permanent form of written communication.

5.4 Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or other breach of contract. Staff should assume that email messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

5.5 Staff should not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform their line manager or the Human Resources Department.

5.6 E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

5.7 To avoid email congestion, staff must refrain from sending trivial messages or copying emails unnecessarily. Employees should delete unnecessary emails regularly, to prevent over-burdening the system. Email which might be required for future electronic reference or transmission should be archived. Hard copies should be taken where a record is required but electronic retention is unnecessary.

5.8 Staff may wish to obtain email confirmation of receipt of important messages. They should be aware that this is not always possible and may depend on the

external system receiving your message. If in doubt, they should telephone to confirm receipt of important messages.

5.9 In general staff should not:

5.9.1 store send or forward private e-mails at work which they would not want a third party to read;

5.9.2 send or forward chain mail, junk mail, cartoons, jokes or gossip;

5.9.3 sell or advertise using our communications systems;

5.9.4 agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. An e-mail is regarded as a signature from the sender in law;

5.9.5 download or e-mail text, music and other content on the internet subject to copyright protection, unless the owner of such works allows this;

5.9.6 send messages from another person's e-mail address (unless authorised) or under an assumed name;

5.9.7 send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure; and/or

5.9.8 be vigilant for email phishing for login or personal information. Not to provide login information and verify emails are from genuine recipients before clicking on links or attached files.

5.10 Staff should return any wrongly-delivered e-mail received to the sender.

5.11 All communication with students must occur using College systems. Staff should be aware that the use of private email and phones may result in allegations by students where the College will not be able to corroborate or help in any defence.

5.12 The College provides students with access to a College email account, Moodle and Microsoft Teams account for communication and passing of work. The College realises that students may have private email accounts and may not wish to use the account provided by the College but should be encouraged where possible to connect the College provided email to their private email to avoid messages being missed.

5.13 On leaving the College, the user account, all email and files in Office 365 OneDrive will suspended immediately and then deleted after one to three months (Managers after three months while all other staff after one month). Any email and files in OneDrive or SharePoint (Teams) needs to be transferred to

other users during the exit procedure. Thirty days after deletion of the user account, any files and email in cloud-based systems, will no longer be recoverable.

6. Instant Messaging

6.1 The College provides both staff and students with instant messaging tools included in the Microsoft Office 365 package (Teams and Yammer) for internal messaging.

6.2 Staff and students should be aware that all messages are monitored and should not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate messages or media. Anyone who feels that they have been harassed or bullied or are offended by material received via Instant messaging should inform their line manager or the Human Resources Department. Students should inform their Personal Tutor.

6.3 Staff should make students aware that this tool is monitored and misuse as set out in 6.2 above could result in disciplinary procedures and possible exclusion from their course.

7. Using the Internet

7.1 The College has a legal obligation to monitor all internet access for safeguarding and the prevent strategy. All students and staff MUST logon using College provided credentials to access the internet (wired or wireless). A failure to do so will be considered by the College to be a failure to follow a reasonable instruction for which disciplinary action may be taken.

7.2 Staff/students should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of the page, or if the fact that our software has accessed the page or file be a source of embarrassment if made public, then viewing it will be a breach of this policy.

7.3 The sites accessed by staff/students must comply with the restrictions set out in this policy. Accessing inappropriate sites will be subject to monitoring and may lead to disciplinary action; it may, in certain circumstances, be treated by the College as gross misconduct leading to summary dismissal.

7.4 Sharing of explicit or inappropriate electronic material by staff/students shall be deemed a breach of this policy and may lead to disciplinary action; it may, in certain circumstances, be treated by the College as gross misconduct leading to summary dismissal.

7.5 The College reserves the right to decline opening websites that are deemed inappropriate and will not be required to provide a reason.

7.6 Social networking sites such as Facebook and Twitter are not restricted in the College and responsibility for controlling use in the classroom remains the responsibility of staff through tools such as LanSchool and MyPC.

7.7 College staff must never engage in political discussions through outside news groups using the College's computer systems. The College is aware that most staff and students have access to and wish to use Social Media websites similar to Facebook and Twitter. Occasional personal use of social media during working hours is permitted, so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.

7.8 Social media sites should never be used for communication between students and staff and should never be used to discuss business or events occurring at the College.

7.9 Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the organisation and create legal liability for both the author of the reference and the College.

8. Telephone Usage

8.1 Reasonable, occasional, private use of the College telephone system is permitted but should not interfere with work.

9. Closed Circuit Television ("CCTV")

9.1 The College may use CCTV to aid security and safety of staff, students and visitors. The College is aware that images and sounds captured on CCTV can amount to "*personal data*" under UK and EU Data Protection Legislation, if an individual can be identified.

9.2 CCTV in public access areas is subject to a new Code of Practice: *Regulation of Investigatory Powers Act 2000*. Staff will be informed that surveillance equipment is being used and why it is being used.

9.3 Cameras are sited where they are clearly visible and must not invade privacy. For example, it would be considered invasive to site cameras in toilets or changing areas. Images captured by CCTV will be subject to restricted access, stored safely and not held for longer than necessary.

9.4 Covert monitoring will only be allowed for the prevention or detection of crime and images contained on these systems will not be held for an extended length of time (defined by the system installed).

10. Cyber Security

10.1 The College is required by the Skills Funding Agency ("ESFA") to be IASME Cyber Essentials accredited. The requirements for this accreditation are set out by the National Cyber Security Centre.

10.2 To comply with the Cyber Essentials accreditation requirements, which may change annually, the College reserves the right to recall any College IT equipment to update or replace as necessary.

10.3 Any IT device (PC, Laptop or mobile) requiring an update to the operating system or software installed, MUST be updated and restarted when requested. Failure to update devices could put the College accreditation at risk and could result in disciplinary action if any device is found to have been prevented from updating to the required level.

11. USB Data Sticks or Pen / Flash Drives

11.1 The College operates a secure Cloud based file storage system and staff and students are required to use Microsoft Office 365 and OneDrive to store and move data where possible.

11.2 The College acknowledges that Microsoft Office 365 and OneDrive may not be suitable for specific types of data and that a USB storage device may be the only alternative. Digital cameras need USB access to download read only images.

11.3 The College may, in certain circumstances, provide a registered USB data storage device for these occurrences. This device MUST be encrypted and have a "Person Identifiable Data ("PID") Disclaimer" form signed and on file with the IT Department (College registered USB device).

11.4 If a College registered USB device is used, staff must ensure confidentiality is always maintained. USB devices may not contain or hold any Person Identifiable Data ("PID") as defined in UK and EU Data Protection Legislation unless approved. Ethical duties of confidence must be observed, and extreme caution should be exercised where PID is being transferred electronically ensuring that all data is fully encrypted to the required standard.

11.5 Any use of non-College USB devices will be allowed under the following conditions:

11.5.1 if unencrypted, may only be used in College as a READ ONLY device and MAY NOT contain any PID or College sensitive information as described in 9.4 above; or

11.5.2 must be encrypted (when prompted and at the user's risk) for any READ WRITE access in the College and MAY NOT contain any PID or College sensitive information without a "Person Identifiable Data ("PID") Disclaimer" form signed and on file with the IT Department.

11.6 Any PID transferred to a Registered USB Device must remain encrypted throughout its journey and must not be transferred to any other internal or external system in an unencrypted form.

11.7 Staff must note and accept that should their encryption password be forgotten by them this will involve reformatting the device and thus a total loss of the data currently stored within it may occur. The Registered USB device must, therefore, not be used to keep data that is not backed-up securely in accordance with the "Information Technology Conditions of Use" policy.

11.8 Encryption software embedded into College registered USB Devices must not be tampered with.

11.9 All USB data devices provided by the College remain the property of the College as does the content on the device. On the termination of employment all College USB data devices are to be returned to the IT Department.

11.10 Any loss of a USB device potentially constitutes a serious breach of the College's security and should be reported to your Line Manager, the Data Protection Officer and recorded as identified in the College data breach procedure.

11.11 Data should always be removed from the USB Device when no longer required.

11.12 For any Personal Information Data ("PID") required to leave the College premises and systems, including via online applications, written permission must first be obtained from the Director of IT or Data Protection Officer.

12. College Laptops, Data Pads and Mobile Devices

12.1 Where staff are issued with a College's laptop, data pad (including iPads) and other mobile devices confidentiality must always be maintained for all PID. NO personal information may be stored unencrypted and it is preferred that this data instead be stored on Office 365 OneDrive and accessed via secure internet.

12.2 Any PID transferred to a mobile device must remain encrypted throughout its journey and must not be transferred to any other external system in an

unencrypted form. It is important to note that some data pads (including iPad's) and some mobile phones cannot be encrypted and therefore staff are prohibited from storing or transferring PID to these devices. All mobile devices including data pads and mobile phones must have a PIN code lock as a minimum security requirement.

12.3 Encryption software embedded into laptops must not be tampered with.

12.4 All College laptops, data pads and other mobile devices and the data they contain are and remain the property of the College.

12.5 Any loss of a laptop, data pad or any other College mobile device potentially constitutes a serious breach of the College's security and should be reported to your Line Manager and the Data Protection Officer and also recorded as an incident in accordance with the Data Breach Procedure.

12.6 Data should always be removed from the laptop when no longer required.

12.7 For any Personal Information Data to leave the College premises and systems, including via online applications, written permission must first be obtained from the Data Protection Officer.

13. Home Working Using College Systems

13.1 The College may allow staff to work from home in certain circumstances where agreed by the Human Resources Department.

13.2 To protect College systems and data (including PID) the College requires that any home private IT equipment used must meet minimum operating system requirements and should be fully updated (authorised patches applied).

13.3 Login to Microsoft Office 365 applications including email, OneDrive and Teams may require signing into Microsoft Company Portal software and will require Multi Factor Authentication (2FA) for access from outside the College.

13.4 Any home private IT equipment used for College business must have up to date and operational virus protection software installed. Failure to have this protection could result in viruses, malware or ransomware affecting College files and data, causing business disruption and reputational damage.

13.5 Where the College deems necessary, staff may be allocated Virtual Private Network ("VPN") access through College firewalls to use IT equipment on College sites from home. The details and credentials for this access may not be passed on to any other person and the College reserves the right to revoke this access at any time. Staff allocated VPN access must follow any security and data security requirements necessary before accessing College systems.

13.6 Any security breach identified by staff working from home must be reported as soon as possible to the Data Protection Officer and also recorded as an incident in accordance with the Data Breach Procedure.

14. Personal use of the College's systems

14.1 We permit the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

14.2 Personal use must meet the following conditions:

14.2.1 use must be minimal and take place substantially out or normal working hours;

14.2.2 personal e-mail must be marked "personal" under the subject header;

14.2.3 use must not interfere with business or office commitments;

14.2.4 use must not commit the College to any costs; and

14.2.5 use must comply with our policies including the Equal Opportunities Policy, Anti-harassment Policy, Data Protection Policy and Procedure, and the Staff Disciplinary Policy and Procedure (Disciplinary Procedure).

14.3 You should be aware that personal use of the College's systems may be monitored (see below) and, where breaches of this policy are found, action may be taken under the Disciplinary Procedure. The College reserves the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use excessive.

15. Monitoring

15.1 The College monitors telephone, e-mail, voicemail, internet and other communications. For business reasons and to carry out our legal obligations in our role as an employer, use of the College's systems including the telephone and computer systems, and any personal use of them, may be continually monitored by the College. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

15.2 To ensure compliance with our rules, policies and procedures (including this policy, Data Protection Policy and Staff Disciplinary Policy) or for any other purpose authorised under the *Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*, staff are required to

expressly consent to the College doing so. This will be done by accepting the terms of use shown on the computer splash screen each time a computer logs onto the College network, or where an iPad or other mobile device is used, by signing a declaration of acceptance of the College's terms of use in the loan form contained in Appendix 2 and Appendix 3.

15.3 A CCTV system monitors the exterior of the buildings and the College's grounds 24 hours a day. This data recorded will be processed in accordance with UK and EU Data Protection Legislation.

15.4 We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

15.4.1 to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

15.4.2 to find lost messages or to retrieve messages lost due to computer failure;

15.4.3 to assist in the investigation of alleged wrongdoing; or

15.4.4 to comply with any legal obligation.

16. Prohibited use of the College's systems

16.1 Access is granted to the internet, telephones and other electronic systems for legitimate business purposes only. Incidental personal use is permissible provided it is in full compliance with the College's rules, policies and procedures (including this policy, the Equality and Diversity Policy, Malicious Communication Policy, Data Protection Policy and Staff Disciplinary Procedure).

16.2 Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. Misuse of the e-mail system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

16.2.1 pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

16.2.2 offensive, obscene, or criminal material or material which is liable to cause embarrassment to the College or its students;

16.2.3 a false and defamatory statement about any person or the College;

16.2.4 material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equality and Diversity Policy or our Dignity at Work Policy and Procedure);

16.2.5 confidential information about the College or any of its staff or clients (except as authorised in the proper performance of a member of staff's duties)

16.2.6 any other statement which is likely to create any criminal or civil liability (for the College or the member of staff concerned); or

16.2.7 material in breach of copyright.

Any such action will be treated very seriously and is likely to result in summary dismissal.

16.3 Where evidence of misuse is found we may undertake a more detailed investigation in accordance with the College's Staff Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

16.4 Any connection of non-college wired IT equipment to the College wired network (excluding the WiFi Bring Your Own Device Network) is prohibited without first contacting the IT Department and could cause a breach of the College Cyber Essentials accreditation. Any such action noted will be treated seriously and is likely to result in disciplinary action.

17. Copyright and Downloading

17.1 Copyright applies to all text, pictures, video and sound, including those sent by email or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate. Copyrighted software must never be downloaded and may not be stored anywhere on College servers.

17.2 The downloading of MP3, MP4 and multimedia files is for the most part copyrighted material. Storage of these files on the disk space provided as home folders is prohibited unless the College holds the license to store and use said files or material and these licenses are held by the IT Department. The College reserves the right to remove any copyrighted material from College servers without notice.

17.3 College employees should not import non-text files or unknown messages on to the College's system without having them scanned for viruses. If you have not been properly trained to scan for viruses, do not import such items at all.

17.4 It is prohibited to install any software not owned by the College onto the network or any computer, iPad or other mobile device belonging to the College. All software licences for any software must be held by the IT Department prior to installation. In addition to Disciplinary Procedure, the College may also take legal action against the offender(s).

17.5 The College reserves the right to confiscate any illegal or unauthorised equipment/software used on College premises. The confiscation period will be for at least one week and may be for the remainder of the academic year. Such illegal or unauthorised equipment/software includes, but is not limited to, the following:

17.5.1 any software that does not belong to the College, or for which the College holds no licence;

17.5.2 any DVD's that contain copies of software, whether or not there are a legal backup of legitimate software; and/or

17.5.3 attached IT related equipment to the network not belonging to the College, with the exception of mobile devices via the wireless network and authorised USB devices (Appendix 2).

18. IT Department

18.1 The IT Department is there to assist you. If you require any information or help about the use or set up of your computer, you should contact the IT Department via the online IT HelpDesk Request System.

18.2 Staff and students will be required to indicate consent to the conditions of use and surveillance referred to in this "Information Technology Conditions of Use" policy, by clicking on an acceptance box within a splash screen, which shall appear on College computers each time they log-on to the College network. This is a statutory requirement and by continuing indicates acceptance of these Conditions and by implication responsibility.

18.3 By accepting the Conditions of Use both staff and students further accept the policies and procedures of the IT Department which are available for staff on the IT Department SharePoint micro site and on Moodle for students in the "Digital & Learning IT User Guide".

18.4 Included in the Service Level Agreement where the Department reserves the right to suspend service to any person who abuses a member of the IT team in any way as defined in the "Policy on Dealing with Malicious Communication".

Appendix 1

Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR) (together known referred to as the UK Data Protection Legislation) and guidance in the Information Commissioner's Employment Practices Data Protection Code.

Monitoring employee use of email and the internet involves the processing of personal data.

The six data protection principles under UK Data Protection Legislation and Part 3 of the Employment Practices Code (monitoring at work) are relevant when monitoring is carried out but some are more significant than others:

1. processed fairly and lawfully (*first data protection principle*);
2. collected only for specified lawful purposes and shall not be processed in a manner incompatible with those purposes (*second data protection principle*);
3. adequate, relevant and not excessive for the purposes for which they are processed (*third data protection principle*);
4. accurate and, where necessary, kept up to date (*fourth data protection principle*);
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; *(fifth data protection principle*); and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). (*sixth data protection principle*);

In respect of the College's compliance with the Employment Practices Code regarding monitoring at work it has regard to the core principles of the Code and the College:

1. recognises that worker's private lives usually extends into the workplace and employees have an expectation of privacy, even where they have been informed monitoring may take place;
2. ensures that appropriate impact assessments are carried out;
3. that its monitoring is justified and proportionate;
4. the need to inform employees that monitoring is to take place; and
5. ensures that only a limited number of staff have access to information obtained through monitoring.

Regulations of Investigatory Powers Act 2000 (RIPA)

RIPA 2000 consolidates a range of law enforcement investigative powers in respect of computer and electronic communications. It regulates certain types of monitoring certain types of monitoring.

Under RIPA 2000 an interception occurs when some or all of the content of a communication is made available during its transmission to a person other than the sender or the intended recipient. This includes any storage of the communication in the telecommunications system before its receipt, such as voicemail that has not been listened to or an unread e-mail.

It is an offence for a person to "intentionally and without lawful authority to intercept…any communication in the course of its transmission by means of either (a) a public telecommunication system or (b) a private telecommunication system.

The lawful interception of communications can however take place if the interceptor has reasonable grounds for believing that both the sender and the recipient have consented to the interception.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)

Businesses can monitor or record communications without consent to:

1. ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business;

2. ascertain or demonstrate standards which are or ought to be achieved by persons using the system;

3. prevent or detect crime;

4. investigate or detect the unauthorised use of the telecommunications system;

5. ensure the effective operation of the system.

Businesses are also allowed to monitor, but not record without consent for the purpose of:

1. determining whether the communications are relevant to the business; and/or

2. monitoring communications to a confidential anonymous counselling or support helpline.

Human Rights Act 1998 (HRA)

Only public authorities are expressly subject to the HRA. The College falls in this category. Article 8(1) of European Convention of Human Rights ("ECHR") states "everyone has the right to respect for his/her private and family life, his/her home and his/her correspondence".

This, however, is not an absolute right and a public authority is permitted to monitor for the prevention of disorder or crime, protection of health or moral and for the protection of the rights and freedoms of others subject to the doctrine of proportionality. The College has regard to its obligations under the HRA and ECHR and is satisfied that the methods chosen for monitoring communications is no more than necessary to accomplish its identified objectives.

Appendix 2 - IT Equipment Loan Form			
Equipment	**Description**	**Quantity**	**Serial Number**

I certify that I have received the above equipment on loan in good condition and working order.

By signing for this College IT equipment I understand that:

1. I am responsible for the safe custody of the equipment at all times. I will be responsible for any accidental damage repair costs not covered by warrantee.

2. The equipment loaned must not be left unattended at any time. In the event of loss or theft of this IT equipment, I must report this to the "Data Protection Officer" immediately. Failure to do so could be regarded as "gross misconduct" as indicated in the "Information Technology Conditions of Use Policy" and could result in disciplinary action.

3. Data stored on this IT equipment MUST comply with UK and EU Data Protection Legislation and may NOT contain any personal or special information unencrypted or approved as described in the "Information Technology Conditions of Use Policy". Failure to comply will be considers gross misconduct could result in disciplinary action.

4. When transporting the equipment between sites or between my home and my place of work by car, the equipment must be secured out of sight in the boot of the car or outside of view.

5. If at any time during the period of the loan I am requested to return the equipment to the College, I must do so without delay.

6. Should I leave the employment of the College prior to the end of the period of loan, I will return the equipment in good condition and working on or before my last day. Failure to do so may result in the value of this equipment being deducted from any final salary payment from the College.

Signed: _____ Print Name: _____

Dated: _____ Department: _____

Appendix 3 IT Mobile Phone Loan Form

Mobile Phone Asset Tag No.	

Name:	
Base Campus	
Department:	
Line Manager:	

Mobile Details:

Mobile Number:		**Tariff Details:**	
Sim Number:		**IMEI Number:**	
Handset Make/Model:			
Other Equipment Given:			

I certify that I have received the above mobile phone on loan in good condition and working order.

By signing for this mobile phone equipment, I understand that:

1. I am responsible for the safe custody of the equipment at all times. I will be responsible for any accidental damage repair costs not covered by warranty.
2. The College negotiates a contract for this device based on role and College requirement.
3. If data is included as part of the mobile phone contract (amount stated above), warnings have been set on the phone. If this warning is ignored or removed, any data charged by the mobile phone contract supplier, will be for the users account and may be recovered from salary.
4. The equipment loaned must not be left unattended at any time. In the event of theft, I may be held responsible for the replacement cost or excess costs (whichever is greater), if during investigation negligence is discovered.
5. No international roaming in included. If the phone is to be taken out of the UK, this must be communicated to IT (including dates) at least one month in advance if international telephone or data roaming is required so that a bolt on can be arranged. The cost for this will be recovered from the user's budget.
6. I will inform the College immediately should the equipment be damaged, lost or stolen and provide a detailed report as to the circumstances of such loss, theft or damage.
7. If at any time during the period of the loan I am requested to return the mobile phone to the College, I must do so without delay including the charger.
8. Should I leave the employment of the College prior to the end of the period of loan, I will return the mobile phone in good condition and working on or before my last day including the charger. Failure to do so may result in the value of this equipment being deducted from any final salary payment from the College.

Loan Out

Signed:		Date:
IT Signed:		

Loan Return

Signed:		Date:
IT Signed:		
Any issues:		