ICT – Information Technology and Communications Policy

No:FIN-IT-POL-001	**Version: 07**
Issue Date: 10/06/2013	**Review Date: 24/05/2023**
Author: Helen Richardson/Martin Herron	**Approved by: Board of Governors**
Equality Impact Assessment (EIA) completed by (name): Helen Richardson	**Equality Impact Assessment (EIA) completed on (date): 29 Jan 2019**

Monitor Changes

Version Level	Details of Change	Date
01	New document	01/11/05
01	New format no change to content	06/02/06
02	Full review, new template and logo	02/07/09
03	Rewrite to amend out of date terms and add greater emphasis to Information Security	10/06/13
04	Full review to include GDPR terms	24/05/18
05	Full review, amended format, no change to content	04/02/2021
06	Timescales for network password changes added	23/2/2021
07	Timescales for network password amended	23-2-2021

01. Aims and Objectives

This Information Technology and Communications Policy ("the Policy") has been put in place by Gateshead College ("the College") and sets out rules for the acceptable use of internal and external electronic mail (email), the Internet, landline and mobile telephones, the College intranet and the College's IT systems generally (together with information on data protection, security and employee monitoring).

The IT software and hardware assets of the College are increasingly diverse and extensive. Remote access from staff and student homes or the premises of third parties is also possible. Access to the College's systems is widespread across a large diverse user population using the College's network (WAN and LAN) infrastructure.

It is therefore of paramount importance for the Policy to protect the interests of users of IT IT and communication systems, including all persons listed in paragraph 3.1 below ("the Users"), and the College, and to ensure that all Users have confidence in the systems provided. The Policy will also assist Users to have access to a reliable and robust system with secure and accurate data.

The Policy also seeks to ensure best practice. It is College policy to perform all information processing and wider IT activities (through local and wide area networking) ethically and in accordance with good business and sector practice.

Policy Objectives

The Policy is central to the use of IT within the college and will:

- Ensure that the College trading and curriculum assets, data and equipment are adequately protected against loss, corruptions, breach of confidentiality and nonavailability.
- Ensure that the interests of Users are adequately protected.
- Ensure an awareness of IT security issues and Information Security issues across the College and within the student body.

02. Scope

The Policy, which is made up of the main Policy document together with its Appendices, forms part of all College employees' terms and conditions of employment.

- The Policy applies to all users of the College's IT and communication systems, including any employee, agent, contractor, staff member, temporary staff member,

student or any other individual having access to or use of electronic facilities, including email, the Internet, fax machines and telephone ("the Users").

- Use of the College IT and communication systems after having been made aware of the Policy constitutes acceptance of the terms of a Policy by a User.
- The Policy applies to all computing systems (hardware and software), telephones (landline and mobile), hand-held computing devices and closed circuit television (CCTV) systems owned, leased, hired, borrowed and managed by the College or for which the College is otherwise responsible or which are managed by third parties on behalf of the College including but not limited to:
    - LANs
    - WANs
    - Fileserver storage
    - Desktop PCs
    - Portable storage media (including mobile devices such as laptops, mobile phones and tablets)
    - Software ○ Peripherals
- The College reserves the right to amend the Policy from time to time to take account of changes in Technology, law and best practice, and will so far as is practicable to do so, bring any amendments to the attention of the Users.
-

Responsibility

The Service Desk Manager is responsible for the monitoring and implementation of the Policy. If Users have any questions about the content or operation of the Policy, they should contact the Service Desk Manager.

Key search words for this document
Data Protection Act 1998, Data, Sharing, Policy, fair, process **Linked Policies – Information Governance and Security Policy GC-POL-003**

03. Relevant Legislation

3.1 The College is bound by a number of legislative provisions to the use of IT.
A brief summary of the main legislative provisions is set out for Users' information.

3.2 **General Data Protection Regulations (GDPR) 2018** The GDPR (2018) makes provision for the regulations of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. There is a Code of Practice (within the Data Protection Act) on the use of personal data in employer/ employee relationships, which shows how the misuse of personal information is prohibited, but also how such information can be used for legitimate purposes. (See also the College Data Protection Guidelines in Appendix 4).

3.3 **The Computer Misuse Act (1990)** This Act was introduced to combat computer hacking, electronic eavesdropping and virus infection. Under this Act, hacking and the introduction of viruses to computer systems are criminal offences. This Act identified three specific offences:

3.3.1 Unauthorised access to computer material (including programs, applications or data).

3.3.2 Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.

3.3.3 Unauthorised modification of material on a computer system.

This Act states that the first offence (the basic offence) is a summary offence punishable on conviction with a maximum prison sentence of six months or a maximum fine of £2,000 or both. This Act states that the second and third offences are triable either summarily or on indictment and punishable by imprisonment for a term not exceeding five years or a fine, or both. These sentences clearly reflect the perceived gravity of the offences. The College takes an equally serious view of hacking or virus proliferation.

3.4 Regulation of Investigatory Powers Act 2000 (together with Regulations pursuant to that Act, including the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000)

This Act prohibits the interception of emails (and telephone calls) without first obtaining the consent of both the sender and the recipient. However, the Regulations enable businesses to intercept telecommunications and emails without the consent of their employees for certain legitimate purposes, including seeking evidence for regulatory compliance, seeking to establish the existence of a fact, detection crime of unauthorised use of the system and ensuring its efficient operation.

3.5 The Human Rights Act 1998

Article 8 of the Human Rights Act 1998 states that:

Everyone shall have the right to respect for his private and family life, his home and his correspondence. However, this right is qualified and may be interfered with in order to protect the rights and freedom of others.

An employer, for example, may claim that by monitoring emails, they are protecting the rights of other employees to have a workplace that is free from discrimination (assuming the employer prohibits the sending of discriminatory material via email). Similarly, the employer may legitimately argue that, by having CCTV they are providing their employees with a safe work environment and further, taking action that is necessary to prevent crime.

04. JANET Acceptable Use Policy

4.1 The College receives Internet and email connectivity via the Joint Academic Network ("JANET") and Users must therefore comply with the JANET Acceptability Use Policy, attached in Appendix 1 of this Policy.

05. Breach

5.1 The College considers the Policy extremely important and wishes to ensure that its IT systems are used legally and in the safest and most effective ways. For this reason, the College will treat any breach of the terms of the Policy by an individual as misconduct, which may result in disciplinary actions being taken against them, in accordance with the College's disciplinary procedure. Where the breach is considered as gross misconduct, this may result in dismissal.

5.1 Any breach of the terms of the Policy by an employee may result in disciplinary action being taken against them, in accordance with the College's disciplinary procedure. A serious breach of the Policy may result in dismissal.

5.2 Any breach of the terms of the Policy by a student will result in the instigation of the student disciplinary procedure.

The College also reserves the right to take steps to recover any losses it incurs through a breach of this Policy from the individual who has committed the breach.

5.3 Any suspected breach must be reported immediately to one of the college's Data Protection Leads (DPL) using the "Report a Data Breach" button on Digital Dash. The GDPR requires that DPLs report any breach to the Information Commissioners Officer (ICO) within 72 hours of the incident.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, those affected must be notified directly except where the following apply:

5.3.1 The Data Controller has implemented appropriate technical and organisational measures to the data affected by the breach to make the personal data unintelligible.

5.3.2 The Data Controller has taken subsequent measures which will ensure that the high risk to the Data Subjects would no longer be likely to materialise.

5.3.3 It would involve disproportionate effort in which case a public communication (or similar) should be made to inform the Data Subjects.

06. Software Licensing and Copyright

6.1 All software must be installed by IT Services Staff unless otherwise expressly agreed with the Service Desk Manager. The loading or running of any unlicensed or unauthorised software is prohibited. Any unlicensed or unauthorised software will be removed and the use of such software may lead to disciplinary action. This prohibition includes screensavers and games.

6.2 Copying of licensed software and programmes by Users is strictly prohibited by the College and may be viewed as copyright theft.

6.3 Users are expected to comply with the Copyright legislation. Copyright may apply to text, music, pictures, and video including materials 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 owner of the material, or an acknowledgement of the original source of the material as appropriate.

6.4 Downloading and installing software from the Internet is prohibited unless it is for legitimate educational use and authorised in advance by the IT department. Users should contact the Service Desk Manager for clarification on particular software if unsure as to its legality.

07. Malware

7.1 All College computers (including all PCs, notebooks, and fileservers) will be installed with the College's approved anti-virus software. At the discretion of the Service Desk Manager, for reasons of technical problem solving, it may be necessary to temporarily suspend the use of anti-virus software.

7.2 All systems publicly visible and accessible via the Internet will be secured as far as is practicably possible in order to maintain system integrity.

7.3 When using the College IT systems, Users must be vigilant. Computer viruses are often sent by email and could cause significant damage to the College systems. If a User suspects that a file may contain malware, they should not open it, but should contact a member of the College IT Services department immediately.

08. Information Security

8.1 Users accepting visitors into the College premises must follow the approved guidelines for visitors and contractors. Visitors must have a bona fide reason for gaining admission to the College premises, and Users responsible for the control of areas containing IT equipment and College information should challenge unauthorised visitors.

8.2 No one may use the College's systems unless they have been authorised and allocated a password by IT Services. The use of College computers by Visitors or unenrolled Students may be granted through the use of one of IT Services' generic Accounts. Passwords for these accounts are randomly generated every 24 hours and can be collected by College Staff from IT Services as and when required.

8.3 Access to information via College systems is allocated to an individual based on their role within the College. This may be student information, financial information or staff information. At all times use of this information must be kept strictly in line with the College's Data Protection Agreement with the Information Commissioners Office.

8.4 All staff are responsible for the security of their network password and therefore access to information under those credentials. Staff should not give their password to others and therefore compromise secure systems.

8.5 Rules stipulating the number of characters that a password should contain and the length of time that a password can be used before it needs to be changed will be published by the IT Services team. These rules may be varied from time to time but the current Password Policy is contained in Appendix 2.

8.6 All Users should log off from their workstation when leaving it unattended.

8.7 No hardware may be connected to the College computer network without the prior authorisation of a member of the College's IT Services team.

8.8 A User's ability to connect to computer systems through the College network does not imply a right to connect to those systems.

8.9 The storage of private data on College systems is prohibited.

8.10 Data may not be stored by Users on College IT systems in encrypted format unless the access keys are made available in advance to the IT Services team.

8.11	The College systems must not be used to break any encryption system or to distribute information on how to break an encryption system of any nature.
8.12	The IT Services team reserves the right to delete any material which contravenes this Policy or otherwise impedes the proper running of the College's system.
8.13	Unless otherwise informed in writing, the IT Services team will delete any files and emails belonging to students within a period of twelve months of their course end date.
8.14	Unless otherwise informed in writing, the IT Services team will delete any files or emails belonging to a member of staff within six months of their leaving employment with the College.
8.15	The downloading of large files, over long periods of time, is discouraged by the College as it may have a detrimental effect on network performance. Disciplinary action may be taken if Users' actions are found to have a detrimental effect on network performance.
8.16	The usage of personal USB sticks and other external storage devices to store personally identifiable data (PID) of any kind is prohibited. The copying of any PID from any college system onto any personal storage device is prohibited.
8.17	Any laptops or storage devices taken offsite regularly and used at locations which are not on the College network must be encrypted by IT Services and signed out using the equipment collection form when collected.
8.18	All Staff must adhere to the College's Policy for the Secure Use of USB Memory Sticks if using external storage devices for holding or transporting data.
8.19	PC Desktops/Documents folders/other local folders should not be used to store data, especially if that data includes any Personally Identifiable Information. The IT Services team will regularly and routinely clear local accounts from PCs on the college network resulting in any and all locally saved files being removed from the local drive of the PC.

09. Email

9.1	The primary use of email by Users at the College must be for work or study. Personal emails are permitted, but must be kept to a minimum, and only outside work time.

9.2	Where access to email is afforded to a User, this may be withdrawn at any time if, at the discretion of the College, it is felt that the User is using email excessively or inappropriately, or to the detriment of their work or study. Acceptable and unacceptable use of email will be determined in accordance with the JANET Acceptable Use Policy, details of which can be found in Appendix 1 to this Policy.
9.3	All Users should be aware that emails can be recovered even after deletion and can be used as evidence in legal proceedings. Emails may be retrieved for ten years after they are sent or received, even where they have been deleted.
9.4	In so far as is permitted by law, the College accepts no liability for the contents of any personal emails sent or received, or for their safe delivery or receipt.
9.5	Users agree to indemnify the College for any losses or consequences arising out of their use of College systems for personal email.
9.6	Email, just like any other form of communication, should reflect the highest standards at all times. Messages should be brief and to the point, and Users should ensure that an appropriate heading is inserted in the subject field. As a general rule, emails should be written in a language that the sender and recipient would be comfortable using in hard copy correspondence.
9.7	In particular, email must not be used to create, transmit, display or store material that is in breach of the College equal opportunities policy, is radically offensive, sexually explicit, biased or discriminatory in any way, offensive, abusive, obscene indecent, threatening, blasphemous, defamatory, false, or a violation or infringement of any other persons copyright or right to privacy.
9.8	Email must not be used in such a way as to cause a waste of time or resources. For example, messages should be distributed only to those individuals or groups to whom they will be relevant, meaningful and useful. Messages should not be sent to large groups when they are irrelevant to many of the persons in the group.

9.9 Use of the College's IT systems is prohibited for the storage, access of dissemination of material relating to any criminal or otherwise illegal activity or unauthorised or unapproved business including:

9.9.1 Personal business transactions.

9.9.2 Forgery or attempted forgery of email messages.

9.9.3 Reading, deleting, copying or modifying of the emails of others.

9.9.4 Sending unsolicited junk mail or chain letters via email.

9.9.5 Using obscene language in emails.

9.9.6 Accessing sending, displaying or downloading offensive messages or pictures.

9.9.7 Sending pornographic or illegal materials as defined by the 2003 Sexual Offences Act.

9.9.8 Sending material likely to cause offence, including discriminatory, harassing or threatening emails.

9.9.9 Violating copyright laws.

9.9.10 Other actions which may bring the College into disrepute.

9.9.11 Disseminating confidential College information without authorisation.

9.9.12 Creating, placing or distributing any advertisement which is of a commercial nature.

9.10 The College ICT Department can arrange to copy any business related emails to the account of another member of the College staff.

10. Internet

10.1 Use of the Internet for legitimate College purposes is encouraged and permitted, where this complies with the JANET Acceptable Use Policy in Appendix 1 and does not contravene any relevant legislation. The Internet must be primarily used for College business and educational purposes. Access is afforded to Users and the College expects all Users to behave in a responsible and professional manner when accessing sites on the Internet.

10.2 Access to the Internet may be withdrawn at any time by a Line manager or student manager if, at their discretion, it is felt that any user is using it excessively or inappropriately, to the detriment of their work or study. There may be certain periods when access to the Internet cannot be guaranteed or will not be permitted.

10.3 Reasonable personal and private use of the Internet is permitted, but should be kept to a minimum and should not interfere with either work or study. Excessive private use may lead to disciplinary action and may, in certain circumstances, be treated by the college as gross misconduct.

10.4

The Internet sites accessed by users must comply with restrictions set out in the Policy and the JANET Acceptable Use Policy. Accessing inappropriate sites may lead to disciplinary action and may, in certain circumstances be treated by the College as gross misconduct.

10.5

Unauthorised use of the Internet is strictly prohibited and includes but is not limited to users accessing, posting, downloading or distributing any illegal, pornographic or other offensive material, unauthorised access to sites or materials (hacking), attempting to disable or compromise the security of information contained on College IT systems, or material in breach of the College equal opportunities policy.

10.6 Internet traffic will be logged and may be monitored or filtered. If disciplinary measures need to be taken against an individual, these logs may be accessed to provide factual information as to which sites have been accessed

10.7 Logs may be accessed in order to obtain information regarding system information but will not be accessed routinely for any other reason. Logs may be accessed if sites are found that have a detrimental effect on system performance or have contravened the Policy.

10.8 Where Internet access is used for private purposes, the College accepts no liability whatsoever for the correct functioning of the service or the materials accessed. The user accessing the Internet agrees to indemnify the College against any action or costs incurred by the College as a result of their private use of the Internet.

10.9 The publishing on the Internet of any information relating to or about the College is only permitted with the prior approval of the Marketing and Communications Department.

10.10 Users must not download or print material (including images, documents and music) from the Internet unless they do so in accordance with a copyright owner's permission. Even if a document is not marked with a copyright notice, the document or otherwise may still be copyright protected. Infringement of copyright is a serious matter which may result in civil or criminal penalties. If users are in doubt, they should not download or print the relevant material.

10.11 Where relevant, any of the rules contained in the Policy applying to the use of email also apply to the use of the Internet, Intranet and internal fileservers and the College IT systems generally.

10.12 All conditions that relate to the use of JANET, the use of email and the Internet also apply to the use of Intranet and internal fileservers.

10.13 Where relevant, any of the rules contained in the Policy applying to the use of email and Internet also apply to the use of voice, telephones, alarms, BMS and video systems.

11. Monitoring and Interception of Data

11.1 The College reserves the right to carry out random checks on user's email or PC sessions for the purpose of safeguarding and for identifying unauthorised use of

11.2 College IT systems.

Staff email content and traffic is not routinely monitored. In view of this, the College expects all users to behave in a responsible manner when using email. The holding of political discussions and the distribution of personal opinions of colleagues and external bodies via email are discouraged. By using College IT systems and thereby accepting the rules contained in the Policy, users are consenting to:

11.2.1 The College monitoring the use of all College IT and communications facilities, including telephone communications, both private and College-related Internet access and email content or traffic if it is deemed necessary for lawful reasons, including disciplinary investigations or to investigate system performance, or in order to comply with a request made by an agency authorised by law.

11.2.2 All email (whether personal or College related) being checked by the College in the event of a disciplinary procedure being instigated in relation to the relevant user.

11.2.3 Emails and voicemail messages (whether personal or College-related) being checked when users are away from the College e.g. due to holiday or sickness absence

It may not always be possible or feasible to obtain the consent of external recipients/ senders of emails. However, monitoring without consent will only occur after the college has taken all practicable steps to inform the relevant individual that the monitoring/ interception is being carried out.

11.3 Users should be aware that email may be received in order to obtain factual information or to comply with obligations under the Freedom of Information Act 2000 or the Data Protection Act. In any event of any user's email communications, Internet access or telephone communications being monitored or checked, the college will endeavour to inform the relevant user that such action is being taken (except where such monitoring or checking is being carried out in connection with the prevention or detection of crime).

11.4 For the purposes of support tasks and maintenance, the IT services team may remotely connect to any college PC in order to assist the current user or perform maintenance duties. Before connecting remotely to another college PC, wherever possible, support technicians will inform any currently logged-on user that any information on the screen will be visible to them (the technicians).

12. Hacking and Computer Misuse

12.1 Users must abide by the terms of the Computer Misuse Act 1990, and in particular, must not:

12.1.1 Use any computer equipment without authorisations.

12.1.2 Try to access information unless specifically authorised.

12.1.3 Modify information on a computer system unless specifically authorised.

12.2 Users may not access the College's system using someone else's user name or password. It is each individual user's responsibility to keep his/her password confidential. Passwords must not be shared.

12.3 No persons outside of the College IT departments may be granted Local or Network Administrator rights on any college equipment. At the discretion of the Service Desk Manager, if a software installer requires that it is executed in a specific user account in order to work, local administrator rights may be temporarily granted to a standard user for the purposes of the installation, then removed immediately after completion.

12.4

Measures to minimise the risk of passwords and/or user accounts being compromised are administered, monitored and controlled by the Network Team. These measures include:

12.4.1 The temporary locking of an account after 5 incorrect password attempts.

12.4.2 Single Login policy – a user account may only log onto one PC on the Gateshead College network at a time. At present this is administered through Impero.

12.4.3 The Network Administrator password must be changed every 12 months. This account is not to be used by any IT technicians unless absolutely necessary.

12.4.4 The password for the Local Administrator accounts on all college PCs must be changed annually during summer breaks.

13. Confidentiality

13.1 The Confidentiality of emails or other communications using the College computer systems cannot be guaranteed. Users must therefore consider carefully whether it is appropriate to send confidential material by email (or otherwise by the College) or to receive the material in this way. Users who are in any doubt should consult the Service Desk Manager.

13.2 Emails incorporating confidential information or personal data must not be disclosed to unauthorised persons.

13.3 Any confidential data, or data including Personally Identifiable Information, sent to third parties via email must be sent using an encrypted, secure mail service. At the time of writing, Mimecast Secure mail is provided to specific members of staff for whom this activity is an essential part of their job.

13.4 All emails will contain a warning and disclaimer. Users should not delete or tamper with that warning and disclaimer.

13.5

The College accepts that its computer systems may be used by Union Members and Officials for the conduct of union business. However, the college cannot guarantee the security of such communications. It is the responsibility of the

Unions to ensure that all data sent or stored on the computer systems complies with all relevant legislation.

14. Housekeeping and Care of Equipment

14.1 The College requires that all computing equipment be treated with care in order to minimise damage, loss of assets or data, and to be properly used for authorised purposes only.

14.2 Users should comply with the guidelines set out in the Care of Equipment Procedure contained in Appendix 3.

15. Remote Access

15.1 The Policy applies to the use of college IT equipment and systems on college premises and elsewhere. Selected users may be able to access the college's systems remotely. In such cases the user shall:

15.1.1 Immediately report any incident which might compromise the system's Security

15.1.2 Avoid the use of the facilities in a public place where possible.

15.1.3 Avoid leaving laptops or portable devices in vehicles overnight.

15.1.4 Avoid leaving usernames and passwords or other security codes in hard copy form with laptops or other portable devices.

15.1.5 Avoid saving any usernames or passwords for any college system in any browser or password management software on any computer/ tablet/ Internet-enabled device

15.1.6 Ensure they log off the virtual desktop system correctly after use. Any accounts found to be left inactive and logged in for 60 minutes will be temporarily disabled by IT Services.

04. Related Documents

Data Classification and Access Control Policy

17 Related documents

Appendix 1 https://community.jisc.ac.uk/library/acceptable-use-policy
Appendix 2 FIN- IT-PRO-007 Password Procedure
Appendix 3 FIN-IT-PRO-009 Care of Computer Equipment Procedure
Appendix 4 GC-GDE-004 Data Protection Guidelines

Other Related documents

GC-PRO-007 Retention and Disposal Procedure FIN-FAC-PRO-002 Mobile Phone Procedure