Board of Management

Finance & Physical Resources Committee

Date of Meeting	**Wednesday 30 September 2020**
Paper No.	**FPRC1-E**
Agenda Item	**3.5**
Subject of Paper	**IT Acceptable Use Policy**
FOISA Status	**Disclosable**
Primary Contact	**Barry Ashcroft, Director of IT**
Date of production	**May 2020**
Action	**For Approval**

Recommendations:

- The Committee is invited to discuss and approve the updated IT Acceptable Use policy

1. Purpose of Report

1.1 The purpose of the report is to provide the Committee with sight of a new draft IT Acceptable Use policy, to enable the implementation of an any agreed amendments prior to publication.

2. Content

2.1 Defining the acceptable use of College IT equipment is key to ensuring that both students and staff understand the risks associated with improper use and provides guidelines for the safe use of technology.

2.2 Using technology safely mitigates the cyber risk to the College by reducing the chances of malicious software compromising network security and inappropriate content being accessed through College systems.

2.3 Students and Staff are provided with guidance on the storage of data within College servers and on both college-owned and personal devices.

2.4 The rationale and necessity for IT resource monitoring and reporting are also defined within the policy.

2.5 The updated policy incorporates GDPR considerations and guidance for staff using personal devices to access College-owned information.

3. Finance & Resource Implications

3.1 There are no financial implications related to approving this policy.

3.2 The effective management and control of IT use mitigates the risk, including the threat of significant disruption due to a cyber security related incident, to the operational success of the College.

3.3 Advising and enforcing defined acceptable IT use mitigates potential operational impact to both students and staff, while upholding the College’s wider reputation.

3.4 An EQIA assessment has been completed for this policy revision.

CITY OF GLASGOW COLLEGE

IT Acceptable Use Policy

Charity Number: SCO 36198

Table of Contents

IT Acceptable Use Policy

1. Introduction

1.1 The College aims to promote the safe and effective use of information technology to facilitate a productive environment for learning and teaching.

1.2 Access to College IT systems and resources is granted subject to the statements set out in this policy. All other College policies apply in the context of the Acceptable Use Policy. All internet access originating from the College network is also subject to the JISC Acceptable Use Policy, which can be found at https://community.jisc.ac.uk/library/acceptable-use-policy

2. Purpose and Aims

2.1 This policy has been created to define the terms of acceptable use of information technology throughout the College.

3. Scope

3.1 Information technology (IT), as referred to in this policy, includes (but is not limited to):

- Computer hardware
- Computer software
- Network services
- Databases
- Digital signage
- Storage devices
- Email
- Telephones
- Instant messaging
- Printers
- Wi-Fi
- All College systems (e.g intranet, Virtual Learning Environment etc.)

3.2 The IT Acceptable Use Policy (AUP) is applicable to all staff, students, visitors,volunteers, contractors and board members. For the purposes of this policy document, these groups will be collectively referred to as '**users**'.

3.3 The AUP applies whether users are using College IT resources on-campus or off-campus.

4. Policy Statement

4.1 Access to resources

4.1.1 Access to IT resources will be granted to currently employed staff, currently registered students, approved contractors and approved visitors at a level appropriate to their work/study requirements.

4.1.2 Access for visitors must be requested through the IT Service Desk in advance. Authorised users **must not** allow visitors to access College IT resources using their own login credentials.

4.1.3 Access to IT resources will cease when a visitor’s business with the College, member of staff’s employment or a student’s course of study ends.

4.2 Conduct and misuse

4.2.1 IT resources are provided primarily to support learning, teaching and College administration. Reasonable personal use is also permitted, provided it does not interfere with College business and complies with this policy.

4.2.2 Users must not use College IT systems to access, send or store unacceptable content. Unacceptable content includes (but is not limited to) content that is:

- Illegal
- Likely to promote illegal acts, goods or services
- Likely to promote terrorism or violence
- Obscene, indecent or pornographic
- Commercially restricted or in violation of copyright
- Likely to cause business or reputational damage
- Defamatory, malicious or abusive
- Offensive
- Likely to bully, harass, victimise or discriminate against another person/group

4.2.3 Users must correctly identify themselves at all times and must not log in as anyone else, or attempt to interfere with audit trails. Users must take reasonable precautions to protect their user accounts.

4.2.4 Users should take reasonable steps to protect their passwords and must not share or disclose them to anyone else. If a device is to be left unattended, users should ensure that the device is locked or that they have logged out.

4.2.5 Misuse of the College IT resources may include (but is not limited to):

- Vandalism or deliberate physical damage to IT equipment
- Unauthorised access to any system or other user's account
- Impersonating another user (e.g. sending messages that appear to originate from another person)
- Sending chain or unauthorised bulk messages (SPAM)
- Misrepresenting the College using a College email account or College branding
- Activities for commercial gain (e.g. running a business, non-College advertising etc.)
- Personal use which incurs a cost to the College (e.g. premium rate telephone calls, bulk printing etc.)
- Using unauthorised or unlicenced software
- Introducing viruses or other malware
- Causing denial of service or impacting system availability by congesting or disrupting College systems
- Breaching or attempting to breach security controls

4.3 Filtering and blocking content

4.3.1 Automated filtering systems are used in the College to protect users and IT systems. However, these systems cannot be guaranteed to remove all unacceptable content. It is, therefore, expected that users will act in a responsible and ethical manner and respect the rights of others when using College IT resources.

4.3.2 Unacceptable content (see previous list) will be blocked for the safety of all users. The extent of this blocking may vary according to location. Also, access to certain IT resources (like the internet or software applications) may be temporarily blocked if necessary. IT will engage regularly with both academic and support colleagues to review and agree internet filter settings to reduce the likelihood of required content being blocked. If users discover content required for College operational delivery (either academic or support) is blocked, access can be requested through the IT Service Desk with a brief operational justification.

4.3.3 Suspicious emails will be held in quarantine and will only be released at the request of the user. Emails and attachments from unknown sources should be treated with extreme caution. If users require any help or advice, they should contact the Operations Helpdesk.

4.3.4 Responsibility for the suitability of content held on College IT systems lies with the author. Users must ensure that all content is appropriate for all other users who may access it, with specific consideration given to young persons.

4.4 Data storage and retention

4.4.1 The College holds and processes information that may be regarded as personal, sensitive or confidential in accordance with the General Data Protection Regulation (GDPR). The principles of GDPR must be adhered to at all times, regardless of whether the user is accessing data on a College-owned or personally-owned device.

4.4.2 Staff should not download or save College-related, personal, sensitive or confidential data to a personally-owned device. If data is downloaded to a personal device for a critical business reason, it must be deleted immediately after it has been used for the purpose it was downloaded for.

4.4.3 The College provides data storage facilities for students to save their work. While every effort is made to ensure the integrity of stored data, the College will not accept liability for loss of any data. Students can also backup critical work to their own personal device\cloud-based storage.

4.4.4 The College is under no obligation to retain student work at the end of a course of study.

4.5.4 Data must be stored in accordance with the Data Protection Act (2018), General Data Protection Regulation (2018) and College data retention requirements.

4.5 Monitoring and privacy

4.5.1 The College reserves the right to monitor all aspects of its IT resources and keep logs of individual user activity. These logs will be used by the College to:

- Detect and prevent malware
- Detect and prevent misuse
- Ensure service efficiency
- Provide data for audit and performance purposes

4.5.2 In accordance with the government's Prevent strategy, the College has a statutory duty to prevent people being drawn into terrorism. Being drawn into terrorism includes both violent and non-violent extremism. The filtering and monitoring of online systems to restrict access to harmful content forms part of this duty.

4.5.3 Data held within College IT systems is not routinely inspected – user data will normally be treated as confidential and private. Inspection of data will only take place in response to an allegation of misuse or to investigate issues related to operational efficiency.

4.5.4 Monitoring may take place under the following circumstances:

- Requests from the police or other authorities
- Requests made under the General Data Protection Regulations (GDPR) or Freedom of Information Act
- Requests to establish facts as part of a misconduct investigation
- Requests from the user themselves
- To facilitate the operation, repair or essential maintenance of IT resources

All monitoring will be subject to relevant legislation.

4.5.5 Users will not necessarily be notified when monitoring and investigatory activity is taking place.

4.5.6 The College recognises that it has a duty to respect the confidentiality of data examined during such investigatory activity.

4.5.7 Student email accounts are provided by Microsoft and, as such, are subject to monitoring as per Microsoft's own terms and conditions, which can be found at https://www.microsoft.com/en-US/servicesagreement/

5. Enforcement and advice

5.1 Users have a personal responsibility to abide by this policy. For less serious contraventions of the AUP, the College will prefer to inform the user and advise of any corrective action necessary. For more serious or repeated contraventions, the College's Disciplinary Policy and Procedures may be triggered. If it appears that user conduct or misuse has resulted in an offence being committed, the College has the right to inform the appropriate authorities.

5.2 While investigating an alleged contravention, the College may restrict or withdraw user access to IT resources. The College does not accept any liability for user losses or expenses resulting from the loss of access rights.

5.3 The co-operation of all users is required to ensure reliable and resilient IT resources. Users who become aware of a suspected breach of this policy should contact the Operations Helpdesk.

6. Legislation

Use of the College's IT resources must comply with existing legislation, including (but not limited to):

- Communications Act 2003
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Counter-Terrorism and Security Act 2015

- Defamation Act 2013
- Equality Act 2010
- Freedom of Information (Scotland) Act 2002
- Investigatory Powers Act 2016
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Telecommunications Regulations 2000
- General Data Protection Regulation (GDPR) 2018

7. References

7.1 Policy Framework

Associated Policies and Procedures	Title
Policy	Social Media
Policy	Use Your Own Device (UYOD)
Policy	Digital Data Security

7.2 Other College Policies and Procedures

Policy / Procedure	Title
Policy and Procedure	Disciplinary
Policy	Equality, Diversity and Inclusion
Policy	Data Protection
Policy	Safeguarding
Policy	Student Bullying and Harassment
Policy	Dignity at Work

7.3 External References

Source	Title

8 Document Control and Review

Approval Status	Draft review	
Approved by		
Date Approved		
EQIA Status	EQIA Conducted?	Yes: ☒ No: □
Proposed Review Date		
Lead Department	Infrastructure	
Lead Officer(s)	Barry Ashcroft	
Board Committee		
Copyright © 2012 City of Glasgow College	Permission granted to reproduce for personal use only. Commercial copying, hiring lending, posting online is strictly prohibited	

9 Revision Log

Version Date	**Section of Document**	**Description of Revision**
Version 1 27 Jun 2012		Initial publication
Version 2 May 2020	All	Full review.