Board of Management

Finance & Physical Resources Committee

Date of Meeting	Wednesday 30 September 2020
Paper No.	FPRC1-F
Agenda Item	3.6
Subject of Paper	Use Your Own Device (UYOD) 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 Use Your Own Device (UYOD) policy

1. Purpose of Report

1.1 The purpose of the report is to provide the Committee with sight of a new draft Use Your Own Device (UYOD) policy, to enable the implementation of an any agreed amendments prior to publication.

1.2 This policy replaces the College Bring Your Own Device (BYOD) policy.

2. Content

2.1 Defining the requirement and expectation of staff that they require access to College-owned information and IT Systems from their personal devices (i.e. mobile phones\laptops\tablets).

2.2 Remind staff of their responsibilities when accessing College-owned data and systems from a personal device.

2.3 Provide safe and secure remote working connectivity for staff using personal devices.

2.4 Define security standards for staff using their personal devices to access College-owned data and systems.

2.5 Defines and clarifies the College as being data owners (Data Controller) of College data, irrespective of data storage location.

2.6 Defines the College being able to withdraw the ability to use personal devices to access College data\systems at any time.

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 system access from personal devices promotes flexible working opportunities for staff who do not have access to a College-owned mobile device and wish to use their own.

3.3 Advising and enforcing minimum security requirements (both software and physical) mitigates potential operational risk and 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.

Use Your Own Device Policy

(UYOD)

Charity Number: SCO 36198

Table of Contents

1. Introduction

Use Your Own Device (UYOD)

1. Introduction

1.1 City of Glasgow College recognises the benefits of a flexible mobile approach to accessing information systems. However, UYOD must be carefully managed to ensure the integrity, accuracy and security of information owned by the college. As such, the purpose of this policy is to inform users of their responsibilities towards information security and management.

1.2 In the context of this policy Use Your Own Device (UYOD) means accessing College IT systems, regardless of location, using a physical device which is not owned and administered by the College.

1.3 The College seeks to promote the effective and secure use of its information systems to ensure a productive environment that supports learning, teaching and allows staff to undertake their duties. The College is responsible for the data which it holds and will manage that data in accordance with all legal and regulatory responsibility in line with other College policies such as, but not limited to, the Acceptable Use Policy (AUP) and General Data Protection Regulation (GDPR) legislation.

2. Purpose and Aims
This policy has been created to:

2.1 Provide guidance to those who wish to use a personally owned physical device to access College systems or information and to inform users of their responsibilities towards information security and management.

2.2 Clearly set out the standards of information security that must be met when using a personally owned physical device to access College systems or data.

3. Scope

3.1. This policy applies to all Users who have been given access rights to College systems and will access the systems on a personally owned physical device.

3.2. Users should be familiar with other relevant City of Glasgow College policies and procedures in the context of UYOD, such as the Acceptable Use Policy and Social Media Policy.

3.3. This Policy has been reviewed by the college Equalities Impact Assessment for positive benefits. The College acknowledges the use of personally owned devices to help meet user's individual needs.

4. Policy Statement

4.1. Device and Data security

4.1.1 The College provides Information Systems such as Office 365 inc. email, Enquirer, Connected and MyCity, which allow secure access to college information using an internet browser. When accessing these systems using a personal device, the device must be kept secure at all times. Users must ensure they log out of their session when they are finished.

4.1.2 Users should be aware that when they access a College system on a personally owned physical device that they are responsible for all aspects of the security of that device. Access to a College system from a free public Wi-Fi service, collectively known as a Hotspot (e.g. free Wi-Fi service on a train), is not recommended as it may not be secure.

4.1.3 Within the College Campuses, users are only permitted to connect a personally owned physical device to the College Eduroam or Guest Wi-Fi networks. In the Student Accommodation Buildings users can physically connect personally owned devices to the data points in their room. No such physical connections of personally owned devices are allowed anywhere else in the College.

4.1.4 Before a personal device is used to access a college system, it is a user's responsibility to familiarise themselves with the device's security features to keep College data secure. As a minimum you must ensure that the device:

- Has up to date anti-virus software installed and running
- Has the latest software updates installed
- Is not modified in a way that the device's manufacturer's security mechanisms are changed, for example 'to jailbreak' the device
- Is secured with a strong password or passcode
- Is, where available, set up with an auto-lock (device locks automatically after an idle time period)
- Is not cached to remember passwords
- Is, where possible, enabled with remote wipe capabilities which ensure that the device can be 'wiped' of all data in the event of loss or theft
- Where available, mobile devices should be enabled with tracking software such Apple's 'Find My iPhone app', Google's 'Find my

Device' or Windows 'Find My Phone', where the device has this feature to enable it to be located in the event of loss or theft

4.1.5 The College takes no responsibility for the maintenance, support or any associated costs with personally owned devices.

4.1.6 As Data Controller, the College retains ownership and control of College data irrespective of device ownership. To this end, co-operation must be given with the IT Team (in conjunction with HR or the Data Protection Officer) if it is deemed necessary to inspect College data stored on your personal device.

4.1.7 College or personal data should not be downloaded to personal devices and accessed via an App (e.g. Citrix or Outlook) or browser. Any College data downloaded to a personal device must be deleted immediately.

4.1.8 The College reserves the right to refuse, prevent or withdraw access to users and/or particular devices/software where it considers that they are unacceptable in terms of security, or other risks, to its staff, students, reputation or system security.

4.2 Network Services (Wi-Fi and fixed)

4.2.1 By connecting to the College network services, all users agree to abide by City of Glasgow College policies and procedures. These include the Acceptable Use Policy and Social Media Policy.

4.2.2 Users must not attempt to breach the security or filtering measures of the College network.

4.3 Legislation

4.3.1 All UYOD use must comply with existing UK legislation and EU directives.

4.3.2 The main laws covering use/ misuse of UYOD are:

- Communications Act 2003
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Counter-Terrorism and Security Act 2015
- Data Protection Act 2018
- Defamation Act 2013
- Equality Act 2010
- General Data Protection Regulation (GDPR) 2018
- Freedom of Information (Scotland) Act 2002
- Investigatory Powers Act 2016
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Telecommunications Regulations 2000

5. Definitions

- **User**: Any person/s that have been given an account and access rights to a college system/s
- **Personally Owned Physical Device**: A device not owned by the college (UYOD) and used to connect to a college system/s regardless of location. A Personally Owned Device may include, but not limited to; smartphones, tablets, laptops, notebooks and PCs
- **Information Systems**: Electronic systems used by the college to provide information to users.
- **College Wi-Fi Service**: Eduroam and City-Guest Wi-Fi networks

6. References

6.1. Policy Framework

Associated Policies and Procedures	Title
Policy	IT Acceptable Use Policy
Policy	Social Media

6.2. Other College Policies and Procedures

Policy / Procedure	Title
Policy	Disciplinary
Policy	Data Protection for Staff
Policy	Data Protection for Students

7. Document Control and Review

Approval Status		
Approved by		
Date Approved		
EQIA Status	EQIA Conducted?	Yes: ☒ No: ☐
Proposed Review Date		
Lead Department	IT	
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	

8. Revision Log

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