Bring Your Own Device Policy

Charity Number: SCO 36198

Table of Contents

Bring Your Own Device (BYOD)

1. Introduction

1.1 Bring Your Own Device (BYOD) means accessing College systems and information through personally owned devices; such as tablets, smartphones, laptops and PCs.

1.2 Traditionally, College systems and information were accessed almost exclusively through College-owned devices, but the rise in the popularity of smart technology means that this is no longer the case.

1.3 City of Glasgow College recognises the benefits of a flexible BYOD approach. However, BYOD must be carefully managed to ensure that standards of information security are not compromised.

1.4 The College seeks to promote the effective and safe use of information systems to ensure a productive environment for learning, teaching and work. The College is responsible for the data which it holds and manages that data in accordance with the Acceptable Use Policy (AUP), the Data Protection Policy for Staff and Students, and the Data Protection Act 1998 (DPA).

1.5 The Data Protection Act sets out the 8 principals of good information handling and clearly sets out the responsibilities for those storing and handling information. As stated in the DPA, the data controller [City of Glasgow College] is responsible for the personal information which it holds. A full overview of the Data Protection Act (DPA) and the College’s associated responsibilities can be found in the Data Protection Policy for Staff and Data Protection Policy for Students.

1.6 The College is fully committed to ensuring that the principles of the AUP and DPA are adhered to, regardless of whether the user is accessing data on a College-owned, or personally owned, device. Any College data stored on a personal device is owned by the College.

2. Purpose and Aims

This policy has been created to:

• Provide guidance to those who wish to use a personally owned device to access College systems or information.

• Clearly set out the standards of information security that must be met when using a personally owned device.

3. Scope

3.1 This policy applies to all support staff, teaching staff, Directors, board members and students who wish to access College systems or information on a personally owned device. For the purposes of this policy, the term ‘user’ applies to any individual who satisfies these criteria.

3.2 Personally owned devices may include, but are not limited to; smartphones, tablets, ipads, laptops, notebooks and PCs.

3.3 All other City of Glasgow College policies and procedures apply in the context of BYOD.

4. Policy Statement

4.1 Data storage

4.1.1 Users must **not** save any College-owned data which may be considered **personal**, **sensitive**, **confidential** or of **commercial value** to personally owned devices.

4.1.2 The College provides information systems such as College email, Enquirer, Connected and MyCity, which allow secure access to data using an internet browser. When accessing these systems using a personally owned device, users should ensure that they log out.

4.1.3 The College reserves the right to clear data stored on any personally owned device which has been used to access College data. This may also result in the removal of any personal data stored on the device.

4.1.4 Users should disable automated, cloud hosted, back-up services on any device which is used to access College data.

4.1.5 Users should clearly separate personal usage and College usage on any BYOD device.

4.2 Data transfer

4.2.1 Users must **not** transfer any College-owned data which may be considered **personal**, **sensitive**, **confidential** or of **commercial value** to personally owned devices.

4.2.2 Any College data transferred via a USB drive should be securely deleted from the USB drive once the transfer is complete.

4.2.3 Cloud storage services are third-party organisations that allow the user to back up files to the internet, which facilitates access from any internet-enabled device. Cloud storage providers include, but are not limited to; Dropbox, OneDrive, Google Drive and iCloud. Users should be fully aware that data stored within these services is being held by a third party. However, ownership of the College data remains with the College and responsibility for data security remains with the user.

4.3 Device security

4.3.1 If personal devices are used to access College data, users must ensure that they are:

- Up to date with anti-virus software
- Up to date with the latest software updates
- Not modified in any way outwith manufacturer guidelines
- Secured with a strong password or passcode
- Set up with an auto-lock (device locks automatically after an idle time period)
- Not cached to remember passwords

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

4.4 Loss, theft or disposal of device

4.4.1 Users must set up remote wipe capabilities, which ensure that the device can be ‘wiped’ of all data in the case of loss or theft.

4.4.2 Users must securely remove all College data when their relationship with the College ends.

4.5 Wireless network

4.5.1 City of Glasgow College offers a logged wireless service (wifi) for users. Connection to the College wireless network requires a valid username and password (the same details you use to log in to any College computer). By using the College wireless network, all users agree to adhere to the Acceptable Use Policy.

4.5.2 Users must not attempt to breach the security or filtering measures of the College network. Users must not download illegal software via this network. If downloading content from the internet, it is the responsibility of the user to ensure that they adhere to the requirements of the publisher, as well as copyright laws.

4.5.3 Users must not physically connect any personally owned device to the College network.

4.6 Data synchroniser

4.6.1 Members of staff may apply to the IT department for their College email account to be synchronised to a personally owned device.

4.6.2 Users should be aware that any synchronised device may be remotely wiped by the College.

4.6.3 If a synchronised device is lost or stolen, users must report this to the IT department immediately.

5. Legislation

5.1 All BYOD use must comply with existing UK legislation and EU directives.

5.2 The main laws covering use/ misuse of BYOD are:

- Copyright, Designs and Patents Act 1988
- Data Protection Act 1998
- Freedom of Information (Scotland) Act 2002
- Malicious Communications Act 1988
- Regulation of Investigatory Powers Act (RIPA) 2000

6. References

6.1. Policy Framework

Associated Policies and Procedures	Title
Policy	IT Acceptable Use
Policy (Draft)	Information Security
Policy	Data Protection for Staff and Students

6.2. Other College Policies and Procedures

Policy / Procedure	Title
Policy and Procedure	Disciplinary

7. Document Control and Review

Approval Status	Approved	
Approved by	Audit Committee	
Date Approved	22 April 2015	
EQIA Status	EQIA Conducted?	Yes: ☒ No: □
Proposed Review Date	2017	
Lead Department	Infrastructure	
Lead Officer(s)	Executive Director Finance	
Board Committee	Audit Committee	
Copyright © 2015 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 1.0		First Version of policy