

## Bring Your Own Device (BYOD) Guideline for Students

### Introduction

Bring your own device (BYOD) refers to the practice of using a personal computing device (computer, tablet, phone, etc.) for learning activities within the College. We recognise that many of our students will have personal devices (laptops, mobiles, tablets) that they will use for learning purposes.

As a College we welcome and encourage the use of student owned personal devices, recognising the significant benefits to learning and teaching and the added flexibility. We also recognise the associated security risks and our responsibilities as a College to ensure the effective and secure use of our information and data systems.

This guidance is designed to allow the use of student owned personal devices in the College in a way that enhances and supports learning. It also aims to protect our students from harm, minimise risk to the College networks and explain what constitutes acceptable use.

This guidance sets out the conditions through which a student may bring their own personal device into College to use for educational purposes and ensure that we manage the data, for which we are responsible, in line with all current legislation including the UK General Data Protection Regulation and The Data Protection Act 2018.

### Devices

#### Student Personal Devices

Students are actively encouraged to acquire and bring their own personal device for both use at home and in the College for which they are solely responsible for.

#### Short-term loan of a device

All campuses have a Lapsafe system with a bank of laptops that are available for short-term self-checkout loans.

#### Long-term use of a device

Where students are eligible for student support funding, the College will follow relevant SFC funding guidance and, where appropriate, a suitable device will be offered to the student to keep. This will either be a laptop, Chromebook, iPad, or other tablet such as an Android device. Students are responsible for the set up and maintenance of their own devices.

Alternatively, students can apply for discretionary funding through the College's online funding application system. If they meet the relevant criteria, funding may be provided to enable them to purchase their own device up to an appropriate maximum value set by the College. Students are responsible for the set up and maintenance of their own devices.

#### On-Site Devices

## Bring Your Own Device (BYOD) Guideline for Students

Students also have access to book a PC in any of the library facilities across the 3 College Campuses.

### Network Access

Students have access to the College's Wi-Fi network with their college user account, or by using the 'Guest' Wi-Fi network. There is also the option to use the Eduroam Wi-Fi network that will allow internet access within the College, but also at many other Colleges, Universities, and numerous Health Boards across the UK. If you are studying at a community venue, these networks are supported by the venue and not Glasgow Clyde College.

### Software

All students will have access to use and/or download the full Office 365 suite of applications including Word, Excel, PowerPoint, OneNote, and Microsoft Teams which can be used on up to 5 devices including mobile phones. This suite will also provide a cloud storage service called OneDrive for securely storing and protecting your files.

### Responsibilities

Students are recommended to obtain insurance for their own personal devices, and to make use of a protective case for transporting their devices to and from College.

Students are solely responsible for any loss or damage to their own personal device(s) that are in use while on College premises. Any damage, loss of data or personal injury resulting from the use of personal devices on the College premises is the responsibility of the individual and not that of the college (see Devices).

The College reserves the right to deny access to the College network to any devices that it deems unacceptable in terms of security or present other risks to the integrity of our systems.

### Support

A video tutorial has also been created to guide students through the setup of their College account: [Setting up your College ICT account - ClickView](#)

Students have access to a level of support whilst using Library ICT facilities, such as:

- On-Campus in-person Student Account Password reset
- Accessing Office 365 - including Word, PowerPoint, Excel, folders, and files
- Using the internet

## Bring Your Own Device (BYOD) Guideline for Students

- Online research tools through Clyde Discover and our subscribed library databases • Accessing Canvas
- Printing, photocopying, and scanning
- Access to a range of computers and course software
- Access to student day-loan laptops at Cardonald and Anniesland Libraries

When students are having issues with their user account and in class, the lecturer is available to assist.

### Compliance

All students must also comply with the JANET Acceptable Use Policy:

<https://community.jisc.ac.uk/library/acceptable-use-policy> as well as the <https://glasgowclyde.instructure.com/courses/30857/pages/student-conduct>

### Recommend Specification

A modern Windows 10, Windows 11 or MAC OS laptop is recommended, as smartphones are not always adequate for the completion of tasks required in class or when studying from home. An iPad or Android tablet device may also be adequate although the recommendation would be to have a separate keyboard to increase the functionality and ease of use.

The recommended specifications for devices are:

- Windows 10 22H2 (If on extended support) / Windows 11 24H2 or above
- Android 13 (Tiramisu) or above
- IOS 18.7.2 (iPhone XS and above)
- MAC OS 14 (Sonoma) or above

### Further Recommendations

- Set and use a strong password or passcode (e.g., pin number or password) to access your device.
- Do not share your passwords or passcode with anyone.
- Have up-to-date anti-malware/virus software installed and running.
- Set your device to lock automatically when the device is inactive for more than a few minutes.
- Take appropriate physical security measures and do not leave your device unattended. □ Ensure your software is up to date e.g., Windows, MAC OS, IOS, Android, Office etc.
- Make use of the Office 365 cloud service OneDrive to store your data as this provides security for all your data.
- Encrypt your device where possible.