cafre
College of Agriculture,
Food & Rural Enterprise

P500 - CAFRE Learner Bring Your Own Device Policy

Issue	Date of Issue	Date of Next Review	Responsibility of	Date approved by CAFRE Education Management Team
2	5 July 2022	30 June 2025	Learner Services Branch	10 June 2024

	CAFRE Quality Manual Index	CAFRE Website (Tick as appropriate)
Document available	√	√

This document can also be produced in alternative formats upon request

P500 CAFRE Learner Bring Your Own Device Policy

Version History

Version	Description of Changes	Date
1	New Policy	July 2022
2	Update in terminology and process. Inclusion of Learner Laptop Loan Scheme.	March 2024

Contents

1. Introduction

CAFRE is committed to providing a safe and secure environment, where learners, can use technology to support their studies and development, whilst being free from harassment, bullying or discrimination. The following policy has been developed to help foster and promote a suitable and secure learning environment. The purpose of this policy is to encourage more widespread adoption of Bring Your Own Device (BYOD) and sets out clearly what is required when using your own mobile device (phone, tablet, laptop etc.) on the CAFRE wireless network. Effective implementation of this policy will minimise the risk of data loss and/or inappropriate use or access to CAFRE electronic resources and information.

BYOD includes personal computing devices, supplied by the learner at their own expense, including, but not limited to, laptops tablets and smart phones. The device can then be used by the student to access learning materials such as library e-books and online lessons.

2. Scope

It is recognised by CAFRE that learners will need to use a range of devices to successfully complete their studies. Many learners find it easier to use their own devices at least some of the time. This policy applies to all CAFRE learners and all authorised users who are provided direct access to our systems or networks. BYO) refers to Users using their own device (which is not owned or provided to them by the college) to access and store college information, whether remotely or typically connecting to the College's Wireless Service.

For the purposes of this policy, such devices include, but are not limited to, smart phones, tablets, laptops, servers, portable hard drives, video and audio recording equipment, any other fixed or mobile computing device. Some devices may not have the capability to connect to college systems. The CAFRE Student IT team are not under any obligation to modify college systems or otherwise assist learners in connecting their own devices to college systems.

3. Objectives

The College's objectives for this policy are:

- The College is responsible for ensuring that Personal Data is properly safeguarded and processed in accordance with the United Kingdom General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018 (collectively referred to in this document as Data Protection Legislation).
- Safeguard the College's information from security threats that could have an adverse effect on its operations or reputation.
- Fulfil the College's duty of care toward the information with which it has been entrusted.
- To establish the rules which govern the use of devices belonging to learners, who are connecting to College systems and services via the Wireless Network.
- The College reserves the right to refuse, prevent or withdraw access to devices where it considers there to be an unacceptable security, or other risk.

4. Technology Enhanced Learning

BYOD will complement existing computer suite facilities at CAFRE. The active use of personal devices for learning in the classroom will be encouraged where Technology Enhanced Learning can be incorporated into the lesson. For example:

- Used to access the internet to research questions and facilitate group work.
- Note Taking (OneNote).
- Interactive lessons and formative assessment (Nearpod, Kahoot etc).

5. User Responsibilities

All individuals who make use of BYOD must take responsibility for their own device and how they use it. When using a mobile device such as a laptop, smartphone, or tablet, whether personal or college owned, to connect to the college network and access college systems and data, you are personally responsible for keeping data secure and must:

- Ensure that you have read and adhered to all relevant policies.
- Familiarise themselves with their device and its security features so that they can ensure the safety of college information (as well as their own information).
- Assist and support the college in carrying out its legal and operational obligations with regard to college data and information stored on your device.
- You are required to co-operate with officers of the college when they consider it necessary to access or inspect college data stored on your device.
- Use the wireless network service provided by the college to access the internet when on college premises.
- Ensure that separate accounts are used on devices shared with family members.
- Ensure that you have installed a suitable anti-virus and malware protection software. For more information about these visit the National Cyber Security Centre's advice page.
- Maintain the device by ensuring both the operating system and additional software (Apps) are regularly patched and upgraded.
- Set appropriate passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device and will be enforced where possible by the College IT Systems.
- Install and configure tracking and/or wiping services, where the device has this feature.
- Take responsibility for any information that is downloaded onto the device.
- Take reasonable steps to prevent loss to their mobile device.
- Ensure that the device is not used for any purpose that would be at odds with the College IT regulations of use especially when it is on site or connected to the College network.
- Maintain the integrity of data and information accessed on the device.
- Seek advice and guidance if you are in doubt about what information you should be storing on your device and how to handle it.

- We have provided each CAFRE user a OneDrive space for encrypted and secure storage. You should use this exclusively for all College related work, including drafts, sharing with teammates etc.
- Keep information stored on a personally owned device to the absolute minimum that is required.
- Ensure that confidential information is not retained on the device for longer than is necessary.
- Avoid internet cafes and other public wi-fi connections as these pose information security risks and should be avoided especially when accessing sensitive college information.
- Ensure that when a personally owned device is disposed of, sold or transferred to a third party all college information is securely and completely deleted.
- MUST NOT attempt to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak' the device.
- While the Student IT team will always endeavour to assist learners wherever possible, the college cannot take responsibility for supporting non-College managed devices.

6. Online Storage

Devices with synchronised online storage present considerable opportunities for data loss or inappropriate use or access to information. Users therefore must ensure the following:

- Where the college has provided OneDrive learners are expected to use this in favour of any other storage option.
- Your college OneDrive should not be synchronised with any other storage solutions.
- No sensitive or important information should be synchronised to or stored on cloud-based storage that has not been provided by the college. This includes but is not limited to:
    - iCloud
    - GoogleDocs
    - Drop box
    - Skydrive
    - SugarSync

7. Removable Storage Devices

Storage mediums and devices such as USB sticks, external hard drives, flash card and any other portable drives carry considerable risks in transporting, storing or transferring information. Removable devices should not be used unless absolutely necessary to temporarily store information. Information on such devices should be retained only long enough to fulfil the specific need. As soon as the requirement is completed the information should be fully deleted and unrecoverable from that device. Encryption should be applied to all such devices.

Learners will not be permitted to plug such a device into a college computer and access will be blocked when attempting to do so.

8. Wi-Fi Restrictions

- Internet access via the CAFRE WI-FI/Student hardwire network is restricted in a similar way to a government network. Certain categories of website are not accessible. Additional sites and categories of site will be added when deemed necessary.
- CAFRE Wi-Fi is subject to the same restrictions as the learner wired network in terms of what can be accessed on the internet, but all the online resources required for learner learning are available. There is no trust relationship between the CAFRE learner network and the learner wireless network therefore learners cannot avail of the CAFRE printing facilities. To print, learners must login onto a CAFRE learner PC.
- Whilst the CAFRE Student IT team provides support for learner access to the campus wi-fi in terms of usernames and authentication, they do not provide support for mobile devices outside CAFRE supplied devices.

9. Procedure for Implementation

If you wish to BYOD to access College systems, data, and information you may do so, provided that you follow the provisions of this policy and the advice and guidance provided through the IT Help Desk.

The College reserves the right to refuse, prevent or withdraw access to users and/or particular devices or software where it considers that there is unacceptable security, or other risks, to its staff, learners, business, reputation, systems or infrastructure.

Technical policies shall be implemented to ensure that certain conditions are met before access to College platforms is provided. These include setting:

- Minimum operating system requirements
- Password compliance
- Firewall requirements
- Antivirus requirements
- Preventing access from unsupported devices

By accessing the wireless network for BYOD the following internet-based services will be made available:

- Internet access in line with college filtering rules
- Virtual Learning Environment - Moodle
- Office 365 including email accounts, TEAMs, and OneDrive access.

Licensed software Applications which are available remotely subject to licensing. Certain services hosted on the internal college network will not be available, including:

- Home drives (H drives)
- College printing facilities
- Specialist software where licensing restrictions apply.

10. Breach of the Guidelines

If any user is found to have acted in breach of these guidelines, they will be dealt with in accordance with the college's Learner Disciplinary Policy.

11. Laptop Loan Scheme

CAFRE recognises that some learners may not be able to access their required online learning since they lack a suitable device or have limited access to a device, such as a laptop or tablet.

In addition to the IT facilities available on campus, CAFRE can also assist learners who require a laptop for their studies and enable them to achieve their academic potential.

The Learner Laptop Loan Scheme provides long and short-term loans of laptops to learners who do not have access to a personal laptop or computer to fully participate in college life.

Learners are advised to speak to their campus Student Support Officer for further information on the Learner Laptop Loan Scheme.

12. Appeals

The learner has the right to appeal a formal decision made by CAFRE. This means that the learner is requesting another individual (or a number of individuals) with the appropriate authority to review the previous decision. The appeal will be considered by an independent Head of Branch, supported by a panel of CAFRE Education Service staff.

The appeal must be submitted:

- Within 10 working days of the decision leading to the appeal; and
- In writing, either by letter or email to CAFREappeals@daera-ni.gov.uk.

CAFRE will aim to notify the learner of the outcome of their appeal within 10 working days of the date when the learner submitted their written appeal.

13. Northern Ireland Public Service Ombudsman (NIPSO)

The decision of the respective appeals panel is final and there is no right to appeal to CAFRE. However, if the learner remains dissatisfied, they have the right to refer the appeal to the Northern Ireland Public Services Ombudsman. Further information about these processes can be found at www.nipso.org.uk.

14. Customer Complaints Procedure

CAFRE is committed to providing its customers with a high standard of service. We welcome comments on the quality of service received and suggestions on how we can improve our service. A customer service complaint is any communication to us, which expresses dissatisfaction with the quality of our service. Complaints regarding the disciplinary process will be considered by an independent Head of Branch. This should be submitted in writing (including dates, times, location of event and staff involved) to CAFREappeals@daera-ni.gov.uk