BYOD (Bring Your Own Device) Usage Policy.

Overall responsibility: Julian Wood	Deputy Principal – Finance and Corporate Affairs
Implementation: Ashok Dave	Department ICT Services
Date issued:	March 2024
Date for review:	March 2025

Endorsed and approved by Date: 12.3.24

Pat Brennan-Barrett
Principal

Contents

1. INTRODUCTION

The purpose of this policy is to establish guidelines for the use of personal electronic devices in the workplace to ensure the security of data/systems and protect the privacy of staff/students and visitors.

The college uses various technologies to support staff and students for ongoing learning and future their careers. The challenge is to get the right balance between appropriate usage in the classroom, and security.

By ‘devices’ we mean laptops/Chromebooks/Tablets/Mobile Phones or any device that can be connected to the internet.

In many cases laptops/chromebooks/tablets will be provided by the college and in these circumstances, students will not be able to use their own laptops/chromebooks/tablets in classrooms or during learning activity.

2. RESPONSIBILITY

Deputy Principal (Finance and Corporate Affairs)

3. SCOPE

This policy is designed to help staff, students and visitors understand College expectations for when and how they can use their own device(s) at the College or accessing the College resources from any location. It sets out clear guidelines on what is acceptable and what is not.

It is expected that the flexibilities the College provides staff and students to ‘Bring Your Own Device (BYOD)’ will be used in the college or if accessing the College resources from any location, in a responsible, ethical, and legal manner.

4. POLICY STATEMENT

We need to provide staff and students with the means and access to the best ICT environment and future opportunities. BYOD can provide flexibility to the user and resource benefits to the College but must be done in a secure and efficient way.

The college allows access to wi-fi by personal devices (BYOD). Access, however, is restricted to ensure the risks to security are mitigated. Where the college provides devices to staff or students, it is expected that these devices will be used for all college-related activities. BYOD use is therefore intended to support students who do not have access to a college device, require access to the college resources from any other locations, and to enhance the student, staff and visitor experience.

Access to the Northampton College wireless network and any college resources, whether with college-provided or personal devices, is filtered and logged in compliance with the Northampton College ICT Acceptable User Policy and the ICT Security Policy. Personal devices must not be connected to the “wired” network.

Access from personal devices is therefore limited to Internet connection only on the wireless network and entails personal responsibility and compliance with all college rules and the Northampton College Acceptable Use Policies.

In using the Northampton College wireless network or any other college resources, users allow ICT Services staff permission to conduct any necessary investigations regarding inappropriate use of the wireless network at any time.

5. DEFINITIONS

The word "devices" will include: laptops, Chromebooks, macbooks, netbooks, smart phones, tablets, eReaders, USB storage devices and any other type of device capable of connecting to the internet or college network or college resources in the cloud.

6. KEY PRINCIPLES

- The college provides BYOD access to the internet via its wireless network where this is necessary for college-related activity and to enhance staff, student and visitor experience.
- The ICT Services Team will provide a robust, secure ICT system environment and an appropriate security monitoring system.
- The College reserves the right to use these systems to monitor correct usage where appropriate.
- Users of the ICT Systems are expected to follow the policies and observe security procedures when using the ICT Systems.
- Disciplinary action may be taken against users not complying with the policy.

7. THE PROCEDURE

A) USAGE OF PERSONAL DEVICE

The primary purpose of the use of personal devices at college is for educational or college business use, where college devices are not available are deemed suitable. The secondary purpose is to enhance the overall staff, student and visitor experience of the College.

Where the college provides a college-owned device for use by staff or students, the expectation is that this device must be used for all college-related activity. Where a college device is not provided to students, the use of personal devices is at the discretion of the College. Where personal devices are used for educational purposes, students must use such devices as directed by their teachers. Usage should not interrupt or distract from educational activity for the student or others using the same learning or communal space.

Anyone bringing their own device is expected to understand how to operate it and use the installed software. Staff should not be expected to give instructions on usage of personal devices.

The use of personal devices is covered by the Northampton College Acceptable Use Policy.

Devices should be fully charged before coming to college and bring own chargers for use when at the College. The College will not provide chargers for personal devices.

Users agree not to attempt to circumvent the college's network security and/or filtering policies. This includes attempting to setup proxies and downloading programs to bypass security.

Students/Staff shall not take photographs or videos without the subject's express permission and agree not to distribute them in any format.

Staff/Students should not take personal images on personal devices or have images of stored on any personal devices. Under no circumstances should live broadcasts be made without express permission from the subject. Staff/Students should not make images of available on the internet, other than the college website, without permission of student/staff/parents/carers and the line manager, as per the Code of Professional Conduct Policy.

Any personal device used on the College premises using the College network or accessing college resources must comply with the following. Any device that does not comply or poses a security risk will be denied access until it is made compliant to meet the below criteria:

- Hardware must be supported by the manufacturer.
- Running latest supported operating system.
- Have the latest security and critical updates applied on the device.
- Where available running a firewall.
- Where available running an antivirus application.
- Not have any inappropriate software running such as Crypto miners, malware etc. which pose significant cyber security risk to college network.
- Not display any inappropriate/offensive messages/visuals.

Students who have been issued a college device are expected to use it for all teaching and learning in college and, for these students, use of personal devices in lessons or other learning activities will not be permitted other than in highly exceptional circumstances.

B) COLLEGE LIABILITY

Users bring their own personal devices to use at Northampton College or access college resources at their own risk and responsibility. It is their duty to be responsible for the upkeep and protection (anti-virus software/security settings) of their devices and to have them charged and adequately insured as appropriate.

College staff may offer help and advice to students and staff in the use of devices where possible but are not responsible for any repair or configuration changes.

C) RESPONSIBILITIES

Northampton College will NOT be responsible for:

- Charging of personal devices or any suspected damage caused by charging.
- Personal devices that are broken, damaged or malfunction while at college or during college-related activities.
- Storage/security of a personal device.
- Personal devices that are lost/stolen/damaged at college or during college-related activities.
- Maintenance or upkeep of any personal device including software updates, hardware upgrades or compatibility issues.
- Any possible device charges to an account that might be incurred during College-related activities e.g. data usage.
- Lost or corrupted data on a device or in any server or cloud storage areas.

ARTIFICIAL INTELLIGENCE

The use of Artificial Intelligence (AI) in the college is guided by principles of ethical use, data privacy, and academic integrity. We are committed to using AI responsibly, ensuring it is used for educational enhancement, and not for plagiarism or other unethical activities. We regularly review our AI usage and stay updated with the latest developments in AI technology to ensure our practices are current and in line with legal and ethical standards.

8. REPORTING

Any breach of the policy should be reported to the Head of ICT services or Deputy Principal – Finance and Corporate Affairs. Where such action is outside of the remit of ICT Services, the Deputy Principal – Finance and Corporate Affairs or the Head of ICT Services will notify the appropriate officer(s) of the College or appropriate authorities.

9. ASSOCIATED POLICIES

- ICT Acceptable Use Policy for Staff
- ICT Acceptable Use Policy for Non-Employed
- ICT Acceptable Use Policy for Students.
- ICT Security Policy
- Data Protection Policy
- Code of Professional Conduct Policy

10. APPROVAL PROCESS

- Policy and Strategy

11. APPENDICES:

Appendix 1: Policy Summary

Appendix 2: Equality & Diversity Impact Assessment

Appendix 3: Data Protection Impact Assessment

Appendix 4. Communication Plan

APPENDIX 1: POLICY SUMMARY

Northampton College allows staff/students to bring their own personal device(s) for educational or college business use in certain circumstances, and to enhance the overall staff, student and visitor experience of college life.

The College will provide the infrastructure and appropriate access needed to use personal devices in a safe and secure way where they are used.

The College may offer help and advice where appropriate but does not provide technical support for personal devices.

The use of personal devices in classrooms will be at the discretion of the tutor/staff.

By using the College network, you agree that the usage will be monitored and recorded in compliance with the ICT Acceptable Use policy and the General Data Protection Regulation.

To assist you in this we recommend you ensure that:

- Your device is fully charged and that you bring your own chargers. The college will not provide chargers.
- Devices should have the latest security patches and antivirus applied.
- You will not take any video or photographs without the express permission of the subject.
- Staff/Students are bound by the College's Acceptable Use policy and do not attempt to circumvent the college's security.
- You only have licenced Software installed on your device.

Northampton College will not be responsible for:

- Charging or any damage caused due to charging while in college.
- Any damage/malfunction caused to the device because of its use in college.
- Any device that has been lost/stolen at college.
- Maintenance/upkeep of personal device.
- Any lost or corrupt data.
- Any financial loss caused because of you using the device on the college network.

Appendix 2: EQUALITY & DIVERSITY IMPACT ASSESSMENT

This template has been designed to help you take action to improve services and practices which affect staff, students and other service users at Northampton College. By completing this template, you would have considered the impact that your policy, practice or service might have on particular social groups within the college community. The exercise will also provide you with the opportunity to demonstrate, where possible, that the College promotes equity, diversity and inclusion.

Once this Equality Impact Assessment has been created, please include on the last page of your policy document.

Policy Details	
What is the policy?	Bring Your Own Device Usage (BYOD)
Is it new or existing?	Existing
Department	ICT Services
Policy Author (postholder title, name)	Ashok Dave – Head of ICT Services
Author of Equality Analysis	Ashok Dave
Date of completion	05/03/2024

Aim and Objectives
Briefly describe the aims and objectives of the policy
To ensure that staff and students understand their obligations when bringing their own device to college (BYOD).

Policy Assessment

Consider whether your policy might have an impact on various groups identified within the categories listed below and explain why you have reached this conclusion.
Please tick (√) the identified level of impact (positive, negative, or no impact) and provide details of your findings.

	Positive Impact	Negative Impact	No Impact	Findings
Race			✓	
Religion and/or belief			✓	
Sex (Gender)			✓	
Gender Identity			✓	
Disability			✓	
Age			✓	
Sexual orientation			✓	
Marriage and/or civil partnership			✓	
Pregnancy and/or maternity (including surrogacy and adoption)			✓	
Other identified group (e.g. carers)			✓	

Action Planning		
How do you intend to mitigate or eliminate any negative impact identified?	If a positive impact is identified, how do you intend to promote or develop this opportunity?	Where negative impact has been identified, can it be justified? If so, explain how.

Monitor and Review	
How will you monitor the impact of your policy once it has been put into effect?	
The policy will be monitored through feedback from services users gathered via: Policy & Strategy.	
Names and position of Impact Assessment Team (min of 3 preferably from areas across the College):	
Name	
Mark Owen	Assistant Principal – Student Services
Mark Poole	Head of Estates
Jane Deery	Vice Principal – School of STEM and Business
Equality Analysis Sign-Off Signature and Date:	*A.V.Dave*
Review Date:	05/03/2024

APPENDIX 3: DATA PROTECTION IMPACT ASSESSMENT

Data Protection Impact Assessment

Does this Policy

- require the collection and use of data in addition that normally collected by the College?

Yes / ~~No~~ (if Yes complete Assessment point number 1)

- require the sharing of data with partners?

Yes / ~~No~~ (if Yes complete Assessment point number 2)

1. Is additional data being collected? If so, please detail:

The college has responsibility to monitor all BYOD connections that go through college Wi-Fi for safeguarding and security reasons.

2. Is data collected personal and/or sensitive?

Yes

3. How will you collect, use, store and delete data?

The data is only stored for 6 months for monitoring and reporting purposes.

4. Will you be sharing data with anyone? Please detail what data, with who and confirm a **Data Sharing Agreement** is in place

Yes only if there is a request from law enforcement. For sharing data with the police, data release form must be sent by them and then signed and agreed by the principal.

5. **Describe the purposes of the processing / sharing:** What are the benefits of the processing/ sharing – for you, and more broadly?

Data is only processed to comply with legal and Janet's acceptable use policy.

6. **Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

Through the various policies.

7. **Describe compliance and proportionality measures, in particular:** What is your lawful basis for processing?

Janet Acceptable Use Policy requires us to be able to identify the device/user in case of serious breach of their policy. This may also be requested by the law enforcement in extreme serious cases.

8. How will you ensure data quality and data minimisation?

The data will as accurate as provided from the device connecting. The data will be kept for 90 days from their last access date and automatically deleted.

9. What information will you give individuals?

User's will be prompted with electronic copy of this BYOD Policy to read and agree annually.

Please attach a Risk Assessment if there are significant risks to data protection.

Signed by Data Protection Officer

Name: Julian Wood

Date: 05/03/2024

Appendix 4: COMMUNICATIONS PLAN

TITLE OF COLLEGE POLICY: Bring Your Own Device Usage (BYOD)	**DATE APPROVED BY** Date: 12/03/2024

AUDIENCE (select appropriate with √)					
Managers	✓	Curriculum teams		Business Support teams	✓
All staff	✓	Suppliers		Partners	
Other – Students	✓				

CHANNEL (select appropriate with √)					
Policy & Strategy Team (PST)	✓	Quality Improvement Network (QIN)		Marketing team	
Meeting		Meeting		NC Update Intranet Website	✓
Individual team		Suppliers		Partners	
Document Library Noticeboards Team meeting Email		e.g. Letter or email Meeting		e.g. Letter or email Meeting	
College Management Team (CMT)		JCNC		CORPORATION	
Meeting		e.g. Meeting Email		e.g. Meeting Email	

COMMUNICATIONS PLAN ACTIVATED BY:		
Name: Ashok Dave Department ICT Services	Job title: Head of ICT Services	Date: 12/03/2024

Appendix 5 : BYOD DEVICE CATEGORIES 2024/2025

The College expects staff/students to use college issued devices, in line with this policy, where these are issued.

For the academic year 2023/24, subject to affordability and availability of suitable devices, the College's approach to the provision of college-owned devices is as follows:

- 16-18 Study Programme students: all students will be issued with either a Chromebook or Laptop as follows:
    - Entry level, Level 1 and Level 2 students – Chromebook
    - Level 3 students (all years) – Laptop or Chromebook subject to availability and course requirements

  16-18 students are not therefore expected to use personal devices for college activity. Students may connect personal devices to the College's wireless network while on campus for personal use in line with this and other college policies.

- Apprenticeships: Apprentices are allowed and expected to use personal and/or employer owned devices. Where this is not possible and/or in cases of hardship or risk to learning the College may provide a device on an exceptional, case by case basis.

- Adult Students (19+ yrs.): Adult students are allowed and expected to use personal devices. Where this is not possible and/or in cases of hardship or risk to learning the College may provide a device on an exceptional, case by case basis.

- HE Students: Adult students are allowed and expected to use personal devices. Where this is not possible and/or in cases of hardship or risk to learning the College may provide a device on an exceptional, case by case basis.

- Students with High Needs: Where appropriate, students with an EHCP or other assessed need will be provided with a college device irrespective of age. In cases of hardship or risk to learning the College may also provide a device on an exceptional, case by case basis.

- College Visitors: Visitors are allowed to use personal devices to connect to the college wireless network.

- Staff: All college staff have access to college owned equipment (laptops) for use at college and, where relevant, when working from home. Staff are expected to conduct College business on these devices. Staff are allowed to connect personal devices to the College network for work purposes (including mobile phones) where this is necessary, and to connect personal devices to the network while on campus for use in line with this and other college policies.

- Students with special written dispensation from the relevant Vice Principal.

**** Any personal devices will only be allowed to connect to the college WiFi and not the wired network.**