BYOD (Bring Your Own Device) Usage Policy 2026-2027

Overall responsibility:	Executive Director Improvement, Skills & Innovation
Implementation:	Director of ICT Services
Date issued:	August 2026
Date for review:	August 2027

Endorsed and approved by: Digital, Data and Systems (DDS) Strategic Implementation Group

Date: August 2026

Jason Lancaster

Principal and CEO



Contents

1. INTRODUCTION 3
2. RESPONSIBILITY 3
3. SCOPE 3
4. POLICY STATEMENT 3
5. DEFINITIONS 4
6. KEY PRINCIPLES 4
7. THE PROCEDURE 4
A) USAGE OF PERSONAL DEVICE 4
B) COLLEGE LIABILITY 6
C) RESPONSIBILITIES 6
8. REPORTING 7
9. ASSOCIATED POLICIES 7
10. APPROVAL PROCESS 7
11. APPENDICES: 7
APPENDIX 1: POLICY SUMMARY 8
Appendix 2: EQUALITY & DIVERSITY IMPACT ASSESSMENT 10
APPENDIX 3: DATA PROTECTION IMPACT ASSESSMENT 12
Appendix 4: COMMUNICATIONS PLAN 14

1. INTRODUCTION

The purpose of this policy is to establish guidelines for the use of personal digital devices (defined in Section 5) in college premises to ensure the security of data/systems and protect the privacy of staff and students and visitors.

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

Northampton College recognises that personal digital devices are an important part of modern learning, communication and accessibility. The Bring Your Own Device (BYOD) approach supports flexible learning, enabling students to access digital resources beyond the classroom.

2. RESPONSIBILITY

Overall Responsibility: Executive Director Improvement, Skills & Innovation
Policy Owner: Director of ICT Services
Operational Enforcement: ICT Services
Student Behaviour Enforcement: Curriculum Teams & Student Services
Staff Compliance: Line Managers
Safeguarding Oversight: DSL / Safeguarding Team

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

College aims to provide staff and students with the means and access to the best ICT environment and resources, now and in the future. BYOD provides 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 managed and, where appropriate, restricted to ensure risks to safety and security are mitigated.

Access to the Northampton College wireless network and any college resources is filtered and logged in compliance with the Northampton College ICT Acceptable Usage Policy and the ICT Security Policy. Personal devices must not be connected to the "wired" network.

Personal devices will normally be restricted to internet access and approved cloud-based college services (for example Microsoft 365, the VLE, and other externally hosted learning platforms). Personal devices will not have direct access to internal college systems or servers

In using the Northampton College wireless network or any other college resources, users acknowledge and accept that ICT Services may need to conduct investigations regarding inappropriate use of the wireless network at any time.

5. DEFINITIONS

Personal devices include laptops, tablets, Chromebooks, Macbooks, Netbooks, smartphones, smart watches, smart glasses, wearable cameras, AI-enabled headphones or earbuds, fitness trackers, augmented reality (AR) devices, virtual reality (VR) devices, and any other device capable of recording, transmitting, processing or storing information or connecting to College resources.

6. KEY PRINCIPLES

- The college provides BYOD access to the internet via its wireless network where appropriate 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.
- The college reserves the right to refuse access to college networks and systems in the event that users do not follow the requirements set out in this 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, and the secondary purpose is to enhance the overall staff, student and visitor experience of the college.

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 and other staff. 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 will not give instructions on usage of personal devices.

The use of personal devices is covered by the Northampton College Acceptable Usage Policy. By using their personal devices on college premises, users accept the terms of the Acceptable Usage Policy.

Devices should be fully charged before coming to college and bring their 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 set up proxies and downloading programs to bypass security.

Staff and students must not take photographs, personal images, videos of others (staff, students, visitors) on personal devices or have images stored on any personal devices without the subject's express permission. Under no circumstances should live broadcasts, images,

recording be made or distributed without express permission from the subject (student, staff, parents, carers) and the line manager, as per the Code of Professional Conduct Policy. Under no circumstances users should not engage in Cyber bullying, harassment or online abuse.

Mobile phones may be used for:

- Multi-Factor Authentication (MFA)
- accessibility tools
- work-related communication
- accessing authorised college educational platforms

"Non-Compliance & Enforcement"

Failure to comply with this policy may result in restricted access to college systems, disciplinary action, and/or referral to safeguarding, the People and Organisational Development team or external authorities depending on severity.

Minimum Device Security:

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 with these requirements or poses a security risk will be denied access until it is made compliant to meet the below criteria:

- Run a **supported operating system version**
- Have **latest security updates installed**
- Use **device lock (PIN, password, biometric)**
- Use **antivirus or built-in security protection where available**
- Not be **rooted or jailbroken**
- Not run software that compromises security

ICT Services reserve the right to immediately restrict, block, or remove network access for any personal device that poses a security, safeguarding, or operational risk, without prior notice.

Risk Mitigation Process

Personal devices used on the College premises and network will be managed through the following risk mitigation process:

- High-risk device → access restricted immediately
- Medium-risk → user notified and given time to remediate
- Low-risk → monitored

Visitor Access

Visitors may connect personal devices to the College guest wireless network where available. Visitors must:

- Use the guest Wi-Fi network only
- Comply with the College Acceptable Usage Policy
- Not access restricted College systems or student information
- Not photograph or record staff or students without permission

Staff must not store sensitive College data, including student records or safeguarding information, on personal devices in accordance with the Data Protection Policy.

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. It is also their responsibility to ensure that chargers used in the college are safe and in good repair. The college accepts no liability for the damage of users' personal devices on college premises.

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.

ICT Services will not troubleshoot, repair, configure, or install software on personal devices beyond basic connectivity guidance.

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 AND WEARABLE TECHNOLOGIES

- Use or wearing of Artificial Intelligence (AI) enabled smart glasses, smart eyewear, or any wearable device capable of recording, transmitting, analysing, or storing audio, video, images or other data is not permitted. This applies on College premises and during all College activities, and is in place to protect the privacy, confidentiality, safeguarding and security of students, staff, visitors and college information.

The use of Artificial Intelligence (AI) and AI tools 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. Use of AI will be governed by the Artificial Intelligence Policy

Breaches will be treated as:

- Academic misconduct (students)
- Disciplinary matter (staff)

Users should refer to the College's Artificial Intelligence Policy for further guidance.

8. REPORTING

Any breach of the policy should be reported to the Director of ICT Services or Deputy Principal for People and Culture. Where such action is outside of the remit of ICT Services, the Deputy Principal for People and Culture or the Director of ICT Services will notify the appropriate officer(s) of the college or appropriate authorities.

If a personal device that has accessed college systems is lost or stolen, the user must report this immediately to ICT Services. This allows the college to take appropriate steps to protect college data and accounts. ICT Services may revoke access or reset accounts as a precautionary measure.

Policy will be reviewed annually or following a significant incident.

9. ASSOCIATED POLICIES

- ICT Acceptable Usage Policy for Staff
- ICT Acceptable Usage Policy for Non-Employed
- ICT Acceptable Usage Policy for Students.
- ICT Security Policy
- Artificial Intelligence (AI) Policy
- Data Protection Policy
- Code of Professional Conduct Policy

10. APPROVAL PROCESS

Digital, Data and Systems (DDS) Strategic Implementation Group

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 and 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 Usage policy and the General Data Protection Regulation.

Why we monitor: -

- Safeguarding students
- Protecting college systems
- Meeting Legal Duties

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 and 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.

What BYOD does not allow

❌ No access to wired network

❌ No access to internal systems or servers

❌ No storing sensitive College data on personal devices

❌ No bypassing filtering or security controls

❌ No use of AI-enabled smart glasses, wearable cameras or recording devices to capture College information.

❌ **No use of wearable devices that automatically upload recordings, images, transcripts or other College information to external AI services.**

❌ **No recording or live transcription of meetings, lessons, examinations or confidential discussions without permission.**

“Failure to comply with this policy will result in appropriate action in line with College disciplinary procedures.”

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 (BYOD) Usage
Is it new or existing?	Existing
Department	ICT Services
Policy Author (postholder title, name)	Ashok Dave – Director of ICT Services
Author of Equality Analysis	Ashok Dave
Date of completion	20/08/2026

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			P	
Religion and/or belief			P	
Sex (Gender)			P	
Gender Identity			P	
Disability			P	
Age			P	
Sexual orientation			P	
Marriage and/or civil partnership			P	
Pregnancy and/or maternity (including surrogacy and adoption)			P	
Other identified group (e.g. carers)			P	

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
Margot Sauntson	Director of Estates
Ashok Dave	Director of ICT Services
Equality Analysis Sign-Off Signature and Date:	*A.V.Dave 20/08/2026*
Review Date:	20/08/2027

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 3 months for monitoring and reporting purposes.

4. Will you be sharing data with anyone? Please detail what data, with whom 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 to 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 requirements and to comply with 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 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 extremely serious cases.

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

The data will be as accurate as provided from the device connecting. The data will be kept for 3 months from their last access date and automatically deleted.

9. What information will you give individuals?

Users 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: Rav Garcha

Date: 20/08/2026

Appendix 4: COMMUNICATIONS PLAN

TITLE OF COLLEGE POLICY: Bring Your Own Device (BYOD) Usage	**DATE APPROVED BY** Date: 20/08/2026

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

CHANNEL (select appropriate with √)					
Policy & Strategy Team (PST)	P	Quality Improvement Network (QIN)		Marketing team	
Meeting		Meeting		NC Update Intranet Website	P
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: Director of ICT Services	Date: 20/08/2026