William College

Staff Bring Your Own Device (BYOD) Policy

© William College. All rights reserved

Document Version Control	
Document Title	Staff Bring Your Own Device (BYOD) Policy
Version	1
Reviewing Committee	N/A
Approving Committee	Senior Leadership and Management Team
Policy Lead	IT Coordinator
Date of Last Review	April 2026
Date of Approval	May 2026
Date Effective from	June 2026
Date of Next Review	November 2027

© William College. All rights reserved

Table of Contents

1. Introduction 3
2. Scope 3
3. Policy 3
4. Security of Devices 4
5. Roles and Responsibilities 4
   5.1 Approval Request Process 5
6. Compliance 5
7. Policy Review 5
8. Related Policies and Documents 5

© William College. All rights reserved

1. Introduction

The purpose of this policy is to outline William College's approach and requirements for the use of staff personal devices to access information, services, systems and data provided by William College.

This policy forms part of William College's broader information security documentation and should be read alongside related policies and documents.

Staff members can apply to Staff Bring Your Own Device (BYOD) for work purposes on a voluntary basis. All staff approved to Bring Your Own Device (BYOD) are required to follow the requirements of this Policy. Failure to do so may result in disciplinary action in line with the College's policies or, where necessary, removal of access to services provided by the College.

2. Scope

Whilst it is recognised that staff use of personally owned devices for work purposes brings benefits to the College, such devices pose a high security risk as they are not managed by the College. These devices may not be patched, may run inadequate anti-virus software and are likely to be more vulnerable to unauthorised access. Staff are also more likely to have admin rights on their personally owned computer which increases the risks posed from malware. Additionally, the risk of a data leak is increased due to the lack of corporate oversight over device usage and permissions.

This policy applies to staff only and covers any personal devices used to access the College network service, assets and systems managed by William College and used to process business information including emails, Virtual Private Network (VPN) connections, Student Records System and instant messaging. Personal devices include but are not limited to personal home computer, laptops, netbooks, tablets and mobile phones.

The aim of the policy is to ensure that the College complies with data protection legislation and that College information, particularly personal and sensitive information, is protected from unauthorised access, dissemination, alteration, or deletion. It complements and supports the existing Data Protection Policy.

3. Policy

All William College staff members are provided with the electronic devices required to fulfil their role; on top of office-based computers, additional corporate devices might be supplied to some staff members according to role needs and institutional approach to remote working. William College permits employees to voluntarily use their personal devices (BYOD) for work-related purposes; personal use of devices remains optional and will not be mandated by the company. All individuals wishing to use their own devices must adhere to the College's Acceptable Use of IT Services Policy, Anti-Malware Policy, device security requirements and approval request as specified below.

The College reserves the right to revoke system access on personal devices as needed. This policy is intended to protect the security, integrity, and confidentiality of the College's technology infrastructure, as well as any personal or institutional data for which the College is responsible.

Personal devices under BYOD must not allow access to College data to other individuals, including family, friends, or partners. For example, permitting a family member to use a tablet or sharing a home computer login where College emails or documents are accessible is strictly not allowed.

Before selling, transferring, or disposing of a device used for BYOD purposes, this must be communicated to the IT team which will remove remote access to company resources

© William College. All rights reserved

4. Security of Devices

William College enforces strict security measures for personal devices that access its systems. These will be checked by the IT team before granting BYOD permission:

- Multi-Factor Authentication (MFA) is mandatory for remote access to authenticated services and information. Circumventing MFA is a breach of policy and will lead to access revocation.
- Devices must be secured by a passcode, password, or biometric authentication (e.g., fingerprint or face recognition). Devices should automatically lock after a maximum of 15 minutes of inactivity.
- All passwords used must comply with the William College Password Management Policy.
- Rooted (Android) or jailbroken (iOS) devices are strictly prohibited from accessing the College's network.
- Devices must always have security features enabled, including biometric locks, PINs, or passphrases.
- Operating systems and software must be regularly updated (e.g., via Windows Update or App Store).
- Laptops must have their firewalls enabled at all times.
- All devices must have an updated antivirus solution installed that is approved by the IT team.
- If household members share the device, access to the College information must be restricted (e.g., using separate user accounts).

Upon termination of employment, the IT team must be notified by the Human Resources team to remove access to company resources. The College reserves the right to unilaterally remove access to company resources if:

- The device is lost.
- The employee leaves the organisation.
- The IT team detects a data or policy breach, malware, or any security threat to the College systems.

5. Roles and Responsibilities

The Senior Leadership and Management Team holds the authority to approve the BYOD Policy.

Line managers are responsible for making sure their team members are aware of, understand, and implement the policy effectively. They play a key role in policy monitoring and compliance at the departmental level.

All partaking staff members are expected to be aware of the College's responsibilities under this policy, as well as the specific requirements outlined to protect institutional data and infrastructure. Compliance is mandatory, and failure to follow the policy may result in disciplinary action in accordance with the College policies and removal of BYOD authorisation. In some cases, this may include the revocation of access to the College-provided services.

The Assistant HR Manager will communicate as part of standard operating procedure all leavers to the IT team to ensure all permissions are removed.

All costs associated with personal devices used under this policy are the responsibility of the employee. This includes the purchase price of the device, as well as any associated phone or data plans.

© William College. All rights reserved

William College will not reimburse staff members for:

- The cost or partial cost of the device
- Monthly phone or data plan charges
- Roaming charges or any overage fees incurred beyond the employee's personal plan limits

5.1 Approval Request Process

The approval request can be summarised as follows:

- Staff members that wish to use BYOD must request this with their Line Manager and the IT team.
- The IT team will inspect the personal device in line with the technical requirements specified above and will enrol the device onto the company's secure connection solutions. Only technical device security settings will be checked, while respecting device privacy. If the security requirements are met, VPN functionality will be set up.
- Connection with company resources will always be done through a secure VPN connection set up by the IT team on device enrolment, which are a key part of ensuring safe connection between staff personal devices and company resources.
- Upon end of employment, the Employee Relations team will communicate with the IT team to ensure all remote access has been disabled as per Starters and Leavers Checklist.

6. Compliance

Any staff members found to have violated this policy may be subject to disciplinary action in line with the Staff Disciplinary Procedures, up to and including termination of employment. Any criminal behaviour may be referred to the authorities to investigate and process.

7. Policy Review

This policy is reviewed every 18 months by the Senior Leadership Team and may be triggered by legislative changes.

8. Related Policies and Documents

- Acceptable Use of IT Services Policy
- Access Control Policy
- Anti-Malware Policy
- Password Management Policy
- Starters and Leaver Checklist
- Staff Disciplinary Procedures

© William College. All rights reserved