ST BRENDAN'S
SIXTH FORM COLLEGE

Faith in Learning

BRING YOUR OWN DEVICE (BYOD) AND REMOTE WORKING DEVICE POLICY

Revision number	202301
Reviewed by Audit Committee	21/06/2023
Next review date	03/2025
Policy owned by:	Executive Finance Director

Introduction

The benefits of accessing the College’s IT and data systems via personal devices (such as tablets, smartphones and handheld computers), is well understood and welcomed. However, access via personal mobile devices gives rise to increased risk in terms of the security of the College’s IT resources, data, and communications systems through the potential introduction of viruses, worms, spyware, trojans, ransomware, or through the illegal access to and removal of personal data.

The purpose of this policy is to set out what and how devices can be used to access the College’s systems whilst maintaining good security controls, and how those controls include monitoring and how personal devices may be accessed, and data on them retrieved, removed or destroyed, and the action which will be taken in respect of breaches of this policy.

Definitions are set out at Annex A.

Scope

This policy applies to all College staff, students, partners, contractors and governors using a personal mobile device to access the College’s IT systems. It applies to the use of the device both during and outside college hours whilst on or off the College site.

Devices used for merely making phone calls, SMS texting or Multi-Factor Authentication (MFA/2FA) fall outside of the Policy’s scope.

Device criteria

Any personal device or College owned personal device used to access College systems must:

- be supported by its supplier/manufacturer;
- have a current software licence and supported software maintenance;
- have all software patches applied within 14 days of the patch release;
- have strong password protection or Multi-Factor Authentication enabled;
- be fully encrypted;
- run current and updated anti-virus and anti-malware protection;
- have a correctly configured firewall enabled (does not apply to Smart phones).

Should, at any time, the device fall outside of the above criteria it must be immediately withdrawn from the College’s systems.

Users’ responsibilities

Users should ensure they have adequate insurance cover in place to cover the cost of repair/replacement of any device (BYOD & RWOD) in the event of loss, theft or damage.

Users:

- are liable for any damage or injury caused by their personal device or charger;
- must ensure that their personal device and charger is electrically safe;
- should keep their personal device secure at all times;
- ensure that their device is free from defects.

The College reserves the right to:

- monitor and filter internet content;
- require content filtering tools and methods (SSL Inspection) installation onto the device;
- in the event of a complicit breach of GDPR to instruct the device to delete datasets;
- deny access when internet filtering tools are disabled;
- remove access to any person/device as it sees fit and for any reason.

Consequences of non-compliance

Breach of this policy may lead to the college revoking access to college systems, whether through a device or otherwise. It may also result in sanctions up to and including exclusion for students and disciplinary proceedings for staff.

Personal device holders are required to co-operate with any investigation into suspected breach, which may involve providing access to the device and surrendering any relevant passwords and login details.

Liability

The College shall not be responsible for:

- any personal devices that are lost, broken or stolen whilst on the College site;
- any data lost from personal devices;
- the maintenance or upkeep of any personal device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

On termination of employment

Staff leaving the College's employ must ensure that all access to the College's systems and any data relating to the College, its staff and students is removed from the device.

Associated policies:

Data Protection Policy
Code of Conduct
Students' Code of Conduct
Disciplinary Policy
Communication Policy
Safeguarding Policy
IT Acceptable Use Policy
E-Safety Policy

ANNEX A

BYOD/Bring Your Own Device refers to connection technologies for electronic devices not owned by an organisation used to access that organisation’s data or IT services.

College refers to St Brendan’s Sixth Form College

College systems includes any software applications, Cloud applications, Cloud services, User Interactive desktops and Mobile Device management solutions owned or subscribed to by the College e.g. Web applications, Microsoft Office 365, Google Workspace, Mobile Device Management containers, Citrix Desktop, virtual desktop solutions, IP telephony.

MFA/2FA Multifactor authentication (MFA) is a security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. Multifactor authentication combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods.

Personal Device means any mobile device, smart phone, tablet, PDA, laptop, notebook, Chromebook or other device capable of connecting to the College’s IT systems.

RWOD Remote Working Organisational Device, refers to any college-owned electronic device used to access the College’s data or services whilst away from College premises.

User Anyone accessing the College’s IT systems via a personal device