Bring Your Own Device (BYOD) Policy

Version	Date	Changes	Author	Approved By
0.1 Draft	August 2023	New Policy	James Vincent (Cyber Security Manager)	David Nelson (Assistant Director D&IS)
1.0 Approved	4th December 2024	None required	James Vincent (Cyber Security Manager)	Greg McCloskey (Director of D&IS)

Purpose

To describe the conditions under which staff my use their own devices to connect to the Queen's University Belfast network for work purposes. This policy covers mobile phones, tablets, laptops, and any other personal device which could be used to access Queen's University data, systems, or services.

Policy

This policy defines the standards, procedures, and restrictions for users who have legitimate requirements to access the Queen's University Belfast's corporate network using a personal device. This policy applies to, but is not limited to, any personally owned device which accesses stored data, systems and services owned by Queen's University Belfast, and all devices and accompanying media that fit the following device classifications (hereby referred to as BYOD):

- Laptops, notebooks, and hybrid devices
- Tablets
- Smartphones
- Any non-Queen's University Belfast owned mobile device capable of storing corporate data and connecting to an unmanaged network.

This policy addresses a range of threats to, or related to, the use of Queen's University Belfast data, systems, or services:

Threat	Description
Loss of device	Devices used to transfer, or transport work files could be lost or stolen
Theft of data	Sensitive corporate data is deliberately stolen or leaked to a third party (whether for financial gain or not) by an employee
Copyright	Software copied onto a mobile device could violate licensing
Malware	Virus, trojans, worms, spyware and other threats could be introduced to the Queen's domain via a mobile device

Compliance	Loss or theft of financial and/or personal and confidential data could expose Queen's University Belfast to the risk of non-compliance with identity theft and privacy laws

This policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the Queen's University Belfast network.

Who does this apply to?

This policy applies to all Queen's University Belfast employees, including full and part-time staff, contractors and other agents who may seek to utilise personally owned devices to access any organisation data, systems, or services. Such access to this data, system or service is a privilege, not a right, and forms the basis of the trust Queen's University Belfast has built with its staff, suppliers, and other constituents. Consequently, employment at Queen's University Belfast does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Policy Detail

This policy is intended to protect the security and integrity of Queen's University Belfast's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. All users to whom this applies must agree to the terms and conditions set forth in this policy to be able to connect their devices to the network or use them to login to Queen's systems, including those systems hosted in the cloud. If users do not abide by this policy, Queen's University Belfast reserves the right to revoke this privilege.

The following criteria will be considered initially, and on a continuing basis, to determine if a user is eligible to connect a personal device to the Queen's University Belfast network.

- Sensitivity of data the user can access.
- Legislation or regulations prohibiting or limiting the use of a personal device for Queen's University Belfast business.
- Technical limitations
- Other eligibility criteria deemed relevant by Queen's University Belfast Cyber Security Team.

Responsibilities of Queen's University Belfast

- Queen's University Belfast reserves the right to refuse the ability to connect devices to corporate infrastructure. Queen's University Belfast will engage in such action if it feels such equipment is being used in such a way that puts systems, data, users, and anything else at risk.
- Queen's University Belfast's Cyber Security team may inspect devices attempting to connect to the corporate network.

Responsibilities of BYOD users

Access is granted to Queen's University Belfast data, systems, and services on the condition that users read, respect, and adhere to all policies concerning the use of these devices and services.

BYOD users shall, without exception:

- Only connect BYOD to wireless internet services (for example QUB Wi-Fi). BYOD should not be connected to the wired network (for example via an ethernet cable)
- Follow data security best practice and adhere to Queen's University Belfast policies.
- Ensure equipment uses encryption to protect data.
- Ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied to BYOD use.
- Utilise a device lock with authentication, such as a strong password, on each participating device. Refer to the Queen's University Belfast password policy for additional information.
- Ensure that confidential data is not stored on BYOD devices.
- BYODs are kept up to date with the latest security patches.
- BYODs have anti-virus/anti-malware software and have the latest anti-virus signatures.
- Ensure that software on BYODs is appropriately licenced.

Queen's University Belfast reserves the right to:

- Install anti-virus software on any BYOD participating device.
- Limit use of network resources on BYODs.
- Through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the corporate network
- Log BYOD activity while accessing Queen's University Belfast data, systems or services.
- Monitor access to the Queen's University network to record dates, times, duration of access, etc. to identify unusual usage patterns or other suspicious activity, and to identify accounts/computers that may have been compromised by external parties.

Support

Queen's University Belfast is not accountable for conflicts or problems caused by using unsanctioned media, hardware, or software on BYOD.