Bring Your Own Device (BYOD) to Work Policy

Document Control:

Document filename	Bring Your Own Device		
Director Lead	Jon Russell	**Status**	Live
Owner	Jon Russell	**Version**	V02.1
Author	Christopher Pratt	**Version Date**	June 2026
Retention period	Review Annually	**Configuration control**	No
Confidentiality	Private	**Distribution**	Moorhouse Consulting/Customer

16th Floor, Dashwood House, 69 Old Broad St, London EC2M 1QS
+44 (0)20 3004 4482

Version Control:

Version	Date	Notes	Completed by
V01	August 2016	Initial Version	Jon Russell
V01.2	October 2022	Updated	Christopher Pratt
V01.3	November 2023	General updates and Device Based Authentication	Christopher Pratt
V01.4	January 2024	Umbrella updates	Christopher Pratt
v02	September 2025	Added Device Based Management and Conditional Access updates	Christopher Pratt
V02.1	June 2026	Annual review	Ethan Box

Table of Contents:

1. Purpose

This policy applies to all Moorhouse staff and Associates that process data on personally owned devices and covers computers and mobile devices (phones and tablets).

This document sets out Moorhouse''s policy on the use of personally owned devices to process data and forms part of the Moorhouse's Information Security Policy.

Whilst it is recognised that staff use of personally owned devices for work purposes brings benefits to Moorhouse, such devices pose a high security risk to Moorhouse as they are not managed by Moorhouse, may not be patched or running adequate anti-virus software, and are likely to be more vulnerable to unauthorised access. Staff and Associates are also more likely to have admin rights on their personally owned computer which increases the risks from malware. Copying Moorhouse or their client's data to personally owned devices also reduces the ability for Moorhouse to know where their data is stored and makes it harder to comply with relevant legislation.

Moorhouse staff are expected to use their work device where possible and only use their BYOD device to support their productivity, whilst respecting and adhering to Moorhouse Information Security posture.

2. Why do we have a Bring Your Own Device to Work Policy?

Most people use their own personal devices to access work related information and data. In addition to this, some staff may choose to use their own device (including tablets and laptops) alongside, company issued equipment.

Connection to the Moorhouse network is monitored and where a user is using a personal device they will be required to install CyberSmart software to ensure that Moorhouse policies are adhered.
This policy sets out the guidelines and requirements for using any personal mobile device such as a tablet, smartphone, laptop etc. to access the Moorhouse Information, Technology and Communications (ICT) infrastructure and systems.

All employees are given a company laptop. This company laptop is to be used as their primary device.

All associates will use their personal laptop.

3. Device Based Authentication inc. Conditional Access

Device based authentication has been introduced across the entire Moorhouse Estate and this has had an impact on the BYOD Policy. Employees and Associates must have personal devices (mobile, notebooks or laptops) registered with Intune.

Company devices are automatically registered.

All devices that required access to the Moorhouse estate must be registered with InTune (Microsoft Endpoint Manager) to receive a security check and be confirmed as "Compliant" Only BYOD devices marked as compliant may access any information based on the conditional access rules in place.

Device based authentication is limited to a single organisation per device, so if the device is registered with Moorhouse, it may not be registered with a second company for compliance checks, so in the event that you need to access client information on the same device, you will need to make a choice between Moorhouse or the Client to confirm which is more convenient for you.

The purpose of the Device based auth including Conditional Access deployment is to ensure the highest level of security is observed across all devices accessing the Moorhouse Tenancy and its information within. To comply with this, the device must have the following:

- Full Disk Encryption (FileVault / BitLocker)
- Active Software Firewall
- Active Anti-Virus Protection
- Must be running a supported OS from the devices respected manufacturer.

4. Employee Responsibilities

Employees are only permitted to use a personal device to access the Moorhouse ICT systems solely for business purposes and in accordance with all relevant company policies. In addition to the BYOD policy, this includes but is not limited to:

- Email and Internet Use Policy
- Data Protection Policy
- Information Security Management Systems (ISMS) Policy

The company is under no obligation to ensure that an employee's personal device has the appropriate specifications and ability to access the Moorhouse ICT systems. The ability of an employee to use their own personal device may be withdrawn at any time.

The company will not provide technical support for personal devices. Employees are responsible for any upgrade, repair or replacement which may be required.

Any misuse or suspected misuse of a device or violation of this policy should be reported to the Finance & Operations Director.

5. Data Protection

The security of Company data is paramount. This includes data about the Company, our clients and our colleagues which may be confidential in nature. All data processed by a personal device during the course of business or on the company's behalf remains the property of Moorhouse. This includes, but is not limited to, email, voicemail, instant messaging, and internet and social media activities.

In addition to commercial and reputational risks which may result from a lapse in data security, the company must guard against a violation of the Data Protection Act 1998 (DPA). It is one of the principles of good information handling under the DPA that appropriate technical and organisational measures are taken against accidental loss, or destruction of, or damage to, personal data. Personal data is defined as anything which relates to a living individual and from which that individual can be identified. This broad definition covers much of the data we process on a day-to-day basis.

6. System and Device Security

The key to the success of this policy is system and device security. This can be achieved by adhering to the following requirements:

- Ensuring the device has the appropriate technical specifications to connect securely to the Company network, ensuring that the appropriate operating system is in place and is kept up-to-date, and ensuring that anti-virus and anti-malware software is up-to-date;
- Adhering to any guidance provided from time to time by the Finance and Operations Director regarding appropriate use and security requirements;
- A secure password/PIN must be used to lock the device when not in use;
- Personal applications on the device (such as email or social media applications) must never be used to send, receive or publish Company information (with exception of business related content on Twitter, LinkedIn etc. and in accordance with the Social Media Policy);
- Company data must remain on our virtual network;
- Ensuring that the device is not lost or stolen and that you immediately report the theft or loss of any device used for business purposes to the Finance and Operations Director.
- Moorhouse will use a range of service to ensure that Web Filtering, Software and OS, VPN are enabled to ensure that Company policies are enforced.

7. Termination of Employment

You must ensure that all Company data and software is safely, securely, and permanently removed from your device no later than your last day of employment with Moorhouse.

8. Policy Enforcement

Violation of this policy may result in your access to Moorhouse ICT systems using your corporate device and any personal devices being revoked. It may also lead to disciplinary action being taken against you in accordance with the company's disciplinary policies.