MOBILE DEVICE & TELEWORKING POLICY

Contents

1. Policy Statement

This policy sets out the responsibilities of staff in regards to the use of mobile technology wherever they are working, which includes off-site/remote working.

This policy has been developed to ensure all staff who have a requirement to access the company's systems remotely or to use mobile devices, do so securely and without introducing unacceptable risks to both the processing of data and the network.

Due to significant changes to working practice and the development of technology, remote access to systems by QRS staff is now seen as the normal way of working.

Personal devices are not permitted to be used for work purposes other than expressly permitted by the IT Director, whilst ensuring that the device is encrypted (Section 7). This policy applies to all staff who work at the company with legitimate right to access the systems e.g. temporary workers.

2. Principles

Critical business processes rely on easy and reliable access to company information systems. Business needs to be conducted remotely with confidence and confidentiality, especially when dealing with sensitive information. This document sets out the policy for holding, recording, storage, sharing and using information via mobile devices (laptop, smart phone etc) and includes a set of controls that can be applied to reduce risks associated with remote access and agile working.

At all times, the processing of information must be in accordance with Data Protection Act (1998), GDPR (2018) and QRS Information Security Policy, Data Security and Data Protection Policy, Risk Management Policy and all other relevant company policies. Failure by any member of staff of the company to adhere to this policy will be viewed as a serious matter and may result in disciplinary action.

3. Definitions

User
Within this policy, the term 'user' includes anyone who uses the company network, phone or computing facilities to access the network.

Mobile devices
This includes but is not limited to laptops, iPads, smart phones.

Scope of Policy
Ensure the appropriate use of mobile devices including laptops, iPads and smart phones.

Ensure that access to information is conducted in a secure and confidential environment regardless of location.

4. Criteria for the issuing of mobile devices

Users will be eligible to have a mobile device if it is deemed necessary to their role.

5. Replacement mobile devices

QRS expects all users who have been allocated mobile devices to take the utmost care and responsibility for them. If a device is lost or stolen, it should be reported immediately to your line manager or the IT Director. Where appropriate, a police report should also be filed in order to receive a crime reference number.

If a device is broken or faulty, please report this to your line manager or the IT Director. A temporary device may be issued if one is available until the device is repaired.

6. Change of User including termination of contract

On termination of contract, the user must return their device/s including all accessories e.g. charger, power cable, data cable, bag or other item supplied by the company for use with the mobile device.

If there is any damaged or missing equipment preventing re-issuing of the devices, the user may be personally charged where appropriate.

A user who has used their own device, for example to monitor their company emails, must remove the login details to their account on the device and remove any company data (including email inbox) from their device prior to termination of contract or when requested to do so by the Company.

7. BYOD (Bring Your Own Device)

QRS forbids the use of using personal devices unless permission has been granted. Permission may be granted under the following conditions:

1) A personal PC/Laptop used to access company information on the QRS SharePoint must only access such data using a virtual machine, which will be installed by the company. The details of access must not be shared.
2) With the exception of Point 1 Personal PCs/Laptops must not be used to access company information or company emails under any circumstances.
3) The company may grant permission to access company emails using a personal mobile phone. If permission is granted the user accepts the MS Company Portal application/Intune will need to be downloaded which will in turn check that the device meets the company's necessary security standards.
4) Personal mobiles must be kept secure at all times e.g. locking after 2 minutes of inactivity, secure PIN/Password/Biometric login.
5) Users of personal devices accept that the Company reserves the right to send a remote wipe request to the mobile device in the event that it is lost, stolen or its security has been compromised.

8. Conditions and Appropriate Use

Where individuals are using a QRS smart phone for emails or internet usage care must be taken not to incur high level of unnecessary cost such as excessive data charges. Work related calls to UK mobiles and landlines are included within the contract. Chargeable calls should be kept to a minimum and only incurred for work purposes when there is no alternative.

Confidential information must not be discussed in open or inappropriate areas. Care must be taken that screens can not be viewed by other people nor viewable by CCTV camera's.

Mobile devices must have security options enabled such as a PIN and/or a secure password/biometric login. The strength of this security will be automatically checked during the installation and login as part of MS Intune. Devices that fail to meet the security requirements will not be granted access to company information including emails.

Unauthorised software must not be installed on any company equipment, including mobile devices. However, the company accepts that the user may be using a personal smartphone or tablet. Only apps downloaded from a reputable location may be installed e.g. Apple App Store. Staff who have been granted access to company information/emails using their own device accept that the company reserve the right to request that specific apps are deleted/not installed if they are a known threat. Failure to comply will result in immediate withdrawal of access to company information/emails.

Personal confidential information must not be sent via email unless it complies with company policies in regards to data transfer i.e. SharePoint and SFTP are not possible and the file has a strong password.

Users must not use their mobile devices while driving, even with a handsfree kit.

9. Health and Safety

The management of Health and Safety at Work Regulations 1999 require QRS to ensure all information and instruction is provided to conform to the appropriate Health and Safety Legislation and associated Regulations. Since December 2003, it has been an offence to use a handheld device whilst driving. It is the responsibility of the staff member not to use a handheld device whilst driving. If a member of staff uses a handheld device whilst driving, there is a risk of prosecution and penalty charge. QRS are not responsible for any penalty charge or other liability.

Using a hands-free kit can also result in a fine and penalty points, under existing Legislation for failing to have proper control of the vehicle if the driver is distracted or a risk of prosecution for careless or dangerous driving. When on QRS business, staff must not use a mobile device within their car, if you need to make/take a call, pull over and park in a safe place and switch off the engine. Users must not use their mobile phone while driving, even with a hands-free kit. If for any reason, a device becomes damaged in a way which could affect the health and safety of the user (such as a smashed screen), refer to the section *'Replacement mobile devices'* of this policy.

Reasonable costs for screen savers or protective cases can be claimed via e-expenses to protect mobile devices.

10. Commissioning of mobile devices

QRS uses cloud technology and all mobile devices (mobiles and laptops) will be configured using MS Azure and MS Intune. Staff who have been granted email access on a mobile device accept that MS Intune will be used during the install process of downloading the Company Portal and the company reserves the right to remote wipe the device if lost or stolen.

11. Mobile Device Management

QRS uses cloud technology and all mobile devices (mobiles and laptops) will be configured using MS Azure and MS Intune. The technical controls in place are detailed in the document 'Azure and Intune configuration summary' and form an important part of the controls of the QRS ISMS.

12. Security

The user must take all possible precautions to ensure the security of QRS mobile devices is maintained at all times. Devices should be password enabled and encrypted at all times. Mobile devices are frequently stolen – to reduce the risk of this, mobile devices should never be left unattended, and this includes leaving devices locked in an unattended vehicle. All security incidents and weaknesses must be reported to your line manager.

All personal devices that access company emails or information are remotely managed by the company using Microsoft Intune e.g. personal smartphones and tablets must be updated to the latest quality patch updates within 30 days of their release.

Employees using their own device must ensure that operating systems are covered by mainstream support. Any operating system reaching end of mainstream support must be upgraded at least 1 month prior to mainstream support ending.

Smartphones and tablets issued by the company will be iOS devices. If you are granted to use your own Android device, then it is expected that additional security/AV is installed on the device.

A mobile device used for Company purposes should only have apps installed from a reputable app store. Should the Company or employee become aware of an app that represents a security risk then we expect individuals to check their devices and delete the app immediately.

No software should be installed on company laptops/devices without the approval of the IT Director.

All Company laptops should have Windows Bitlocker enabled. No company data with a classification of Business, Staff or Participants Confidential should be saved locally unless there is no alternative as part of the Company's service delivery.

The use of removable media on mobile devices is forbidden for documents/files with a sensitivity label of Business, Staff or Participant Confidential unless permission has been granted by the IT Director or DPO. Where permission has been granted the removable media should be encrypted to at least AES256 standard.

Home workers must ensure that their home router has the default password changed during router set up. Home workers are encouraged to check for router firmware updates on a regular basis.

Workers should not use a public Wi-Fi such as in a coffee shop whilst using a mobile device. Should a member of staff require access using a public Wi-Fi during the course of their business they must only access company information through a company VPN.

13. Private access

Mobile devices issued by QRS should only be used for QRS business. QRS receives itemised bills and data usage on smartphones and tablets and monitors this regularly. Any unusually high usage will be referred to the line manager for review. It is the individual's responsibility to respond to any discrepancies. Staff provided with a mobile phone or tablet may receive bills for personal usage.

14. Responsibilities

All users with remote access and/or use of a mobile device are responsible for complying with this policy and associated standards. All staff must safeguard company equipment and information resources and notify QRS immediately of any security incidents or breaches. All users of information systems, devices and applications via the network must ensure they are aware of and comply with their security responsibilities. Irresponsible or improper actions will result in disciplinary action.

These policies supplement your terms of employment but are not of contractual effect. Their purpose is to explain the Company's current policies and procedures, but they may be subject to change without notice if changes are considered appropriate by the Company or if there are changes in relevant legislation.