Mobile Device Security Policy

1. Introduction

Mobile devices, such as smartphones, laptops and tablet computers, are important tools for the organisation and their use is supported to achieve the goals of the Royal Conservatoire of Scotland.

However, mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organisation's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

The Royal Conservatoire of Scotland has a requirement to protect its information assets in order to safeguard its students, staff, patrons, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

2. Scope

All mobile devices, whether owned by the Royal Conservatoire of Scotland or owned by staff and students, that have access to corporate networks, data and systems. This includes smartphones and tablet computers.

3. Policy

1.1 Technical Requirements

1. The following Operating Systems have been tested Exchange ActiveSync: Android 2.2 or later, iOS 4.x or later. Other devices and configurations may work have not been tested.
2. Devices must be configured with a secure password that complies with the Royal Conservatoire of Scotland's password policy. This password must not be the same as any other credentials used within the organisation.
3. With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

1.2 User Requirements

1. Users of this service agree that their device will be remotely wiped in the event of its loss, theft or on the termination of the employee's contract with the Royal Conservatoire of Scotland. **NB:** Users should take care to back-up their personal files and photos appropriately.
2. Users must report all lost or stolen devices to the Royal Conservatoire of Scotland's IT Department immediately.
3. If a user suspects that unauthorised access to institutional data has taken place via a mobile device, they must report the incident in alignment to the Royal Conservatoire of Scotland's IT Department immediately.
4. Devices must not be "jailbroken/rooted"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
5. Users must not load pirated software or illegal content onto their devices.
6. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source contact the Royal Conservatoire of Scotland IT Department.
7. Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied at least once a month.
8. Devices must not be connected to a PC which does not have up to date and enabled anti-virus/malware protection and which does not comply with corporate policy.
9. Users should be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that institutional data is only sent through the Royal Conservatoire of Scotland's email system. If a user suspects that institutional data has been sent from a personal email account, either in body text or as an attachment, they must notify the Royal Conservatoire of Scotland's IT Department immediately.
10. Users must not use corporate workstations to backup or synchronize device content such as media files, unless such content is required for legitimate business purposes.

*To jailbreak or root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.