**Guidance for Computer Science Staff Member Accessing e-mail from a Mobile Device**

**Date:** 20/11/2013  
**Author/Contact:** Tom Chothia  
**Classification:** Open

**Executive Summary:** This document provides guidance to members of staff in the School of Computer Science who wish to access their e-mail on a mobile device. We recognise that unobstructed access to e-mail is vital to the operation of the school and, in particular, for maintaining the school’s very high student satisfaction levels, grant capture rate and research output. The academics in the School often work away from the office, hence a policy that overly restricts access to e-mail will have a negative affect on both the schools income from grant capture and student satisfaction levels. As a leading UK Computer Science School and a “GCHQ Centre of Cyber Security Excellence”, a security policy that is seen as poorly thought out will have a negative affect on the schools standing and will affect our ability to recruit top staff (especially in the area of security).

Balancing these factors with the need to protect confidential information and the Schools obligations under the Data Protection Act, we make the following recommendations to staff members:

- Use only Android devices, iPhones or iPads to access e-mail,
- Ensure that the phones are protected with a password or access code,
- Ensure that e-mail is only stored in a safe protected area on the phone,
- Turn on GPS location for lost devices, as well as functions to remotely lock and wipe the device.

**Scope:** This document applies to staff members of the School of Computer Science, at the University of Birmingham. It provides guidance only for staff members that do not handle confidential information in their e-mail, and do not expect to be sent or receive any confidential information. We note that the confidential information held by the school of computer Science is described in the document: “Confidential Information Held by the School of Computer Science” and none of this information should be sent by e-mail.

**Related Documents:** “Confidential Information Held by the School of Computer Science”, School of Computer Science, University of Birmingham.

**Version History:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20/11/2013</td>
<td>1.0</td>
<td>Tom Chothia</td>
<td>Initial version</td>
</tr>
<tr>
<td>6/1/2014</td>
<td>1.1</td>
<td>Tom Chothia</td>
<td>Minor edits</td>
</tr>
</tbody>
</table>
Recommendations:

**Device Type and OS:**

Staff members should use a device running Android Version 3 or higher, or an iPhone or iPad updated to the latest version of the OS. These devices and OSs offer full disk encryption and will protect access to the e-mails. Only the standard Android and iPhone application should be used to access e-mail (unless a third party application is explicitly recommended by IT Services). The default mail applications are publically documented and have the advantage of being inspected by a wide range of independent security professionals; therefore we can have some certainty that they do actually offer the security they claim.

*Action required by the user:* Verify the type and OS of your device, when possible update the device OS via the settings menu.

**Device Password:**

The user's device should be locked with a password or access code. The device should automatically lock after a period of inactivity. The device should refuse to accept passwords after a small (less than 10) number of incorrect tries. The device should then only be unlockable when connected to a paired desktop computer, from confirmation via e-mail, or some other second factor authentication method.

We note that a short access code is acceptable. The important feature is the lock out after a small number of failed attempts. The University's infrastructure allows an attacker to make tens of thousands of guesses of username and password guesses, therefore the level of security of an access code and a lock out is a stronger level of security than University users currently have. Requiring a complex password on a device without a keyboard will lead to users disregarding the password advice and so lead to a lower overall level of security.

*Action required by the user:* To enable these settings the user should set a password or access code on the settings menu on their device. The time out and lock out after failed attempts are automatically enabled, and should not be turned off.

**Location of Downloaded e-mail:**

E-mails downloaded to the phone should only be stored on the internal memory of the device (i.e. not on removable memory). Third party applications should not be granted access to the e-mails. This has the advantage of storing the e-mail in a protected area of the phone.
Action required by the user: None. The requirements of this section are the default settings on the devices listed above and do not require any configuration from the user. However, the user should not reconfigure their device to store e-mails on a removable memory card, or grant third-party applications permissions to access e-mail.

Remote GPS Location and Wiping of Lost Devices:

Users should ensure that remote wipe, remote lock (lost mode) and GPS location are enabled on their devices. On discovering that a device is lost the user should immediately attempt to locate it via GPS and put the device into lost mode. If the device is not found within 24 hours the user should wipe it.

Action required by the user: To enable these settings for Android: go to the "Google Settings" app on your phone, click on "Android Device Manager" and then click "Allow remote factory reset". You can then log into Android Device Manager https://www.google.com/android/devicemanager and manage the settings from there. For iPhone or iPad: go to "Settings" on your phone, then "iCloud" and turn on "Find my iPhone". The phone can then be found and wiped via iCloud. (https://www.icloud.com)

Verification of Settings

We note that it is not possible to remotely verify the security configuration of a mobile device without complete control of the hardware. There is no product on the market that can do this; any claims along these lines are incorrect and usually based on the unrealistic assumption that the users will not install any other mail client on their phone. Therefore our policy accepts the risk that users may refuse to correctly configure their devices. However, the University may ask users to present their devices to University staff in order to check that the devices are properly configured at the time of inspection.