University of Aberdeen Mobile Devices: Advice and Tips

Cameron Muir. Reviewed September 2014.

This document provides advice on how to get the best from your University mobile device, and how to proceed if your device is lost, stolen or damaged.

Reduce costs

Our mobile device tariffs comprise the cost of voice calls and the cost of data transfer.

- Voice calls are charged per minute. The contract with our network provider does not include free minutes, so you will be charged for each phone call you make or text message you send.
- Data contracts include a generous monthly data allowance for use within the UK and on our provider’s network. If you exceed the data allowance, or if you use your device for data transfer while abroad, the resulting bills can be substantial.

The data allowance should more than cover normal day-to-day e-mail and calendaring. To minimise data charges in the UK, avoid large downloads (your device will not download e-mail attachments unless you tell it to do so), extensive web browsing and streamed data, especially video.

While it is possible to use some mobile devices as laptop modems (tethering), this should be avoided unless absolutely necessary. Use a dedicated USB broadband modem instead; this will have a more generous data allowance.

For information on tariffs and data allowances, see:

www.abdn.ac.uk/it/documents-uni-only/UoA-corporate-devices-tariffs.pdf

Travelling Abroad

Using mobile devices abroad can result in extremely large bills; however, there are steps you can take to help minimise costs. For guidance on how you can prepare your University mobile device for use outside the UK, see our fact sheet Travelling Abroad with Mobile Devices.

Improve battery life

There are a number of things you can do to improve the battery life of your device:

- Reduce the brightness of the screen.
- Avoid overusing wireless, Bluetooth and GPS; they will consume large amounts of battery power even when “idling”. Switch them on only when you need them.
- Similarly, only use push e-mail and calendaring when you need it. Set up scheduled or manual synchronization outside business hours instead.
- Set your device to turn the screen off after a few minutes of inactivity.
- Use the mains adapter, whenever it is practical to do so.

What to do if your device is stolen, lost, or damaged

If you believe that your University mobile device has been stolen or lost:

- Contact the IT Service Desk on 01224 27 3636 as soon as possible. The Service Desk will arrange for it to be barred as a matter of urgency.
- You can also remove potentially sensitive data from the device by wiping e-mail, calendar and contacts remotely from any internet-connected PC:
  - Log into Outlook Web Access: https://outlook.com/owa/abdn.ac.uk
  - Click on the cog icon (top right)
  - Select Options
  - Select Phone from the list on the left of the screen
  - Select Mobile Devices
  - You will be presented with a list of devices which have connected to your Exchange account; most users will only have one. Devices are listed with the most recently connected device at the top of the list.
  - Identify the lost device and select it.
  - Click on the Wipe device icon
  - Click on OK to confirm.
  - The device will now be labelled Wipe Pending. You will receive an e-mail once the wipe is complete.
Please note: The wipe will not happen if the lost device is switched off or otherwise unable to communicate with the internet.

- If a lost device is subsequently recovered, please contact the DIT Service Desk on 01224 27 3636. They can authorise its reactivation.

If your device is damaged:
- Contact the IT Service Desk on 01224 27 3636. They will assist you in arranging a repair or replacement.

What to do if your device is not synchronizing

If you suspect that your phone is not synchronizing e-mail or calendar information correctly, there are a number of quick things you can do to resolve the issue.

- Ensure that the time and date on the device are correct and that it is set up for the appropriate time zone.
- Attempt a manual synchronization. Open Activesync and click on Sync. Synchronization should complete within a minute or so.
- Restart the device. If it will not power down and there is no obvious restart button, remove the battery for a few seconds.

If the device still is not synchronizing, switch it off (remove the battery if necessary) and report the fault to the IT Service Desk on 01224 27 3636.

Security

Ideally, you should not store confidential data on a mobile device. The recommended solution for transporting potentially sensitive data is to use an encrypted USB data stick.

We recognise, however, that a significant amount of your e-mail could be regarded as sensitive. To help prevent unauthorised access, the University e-mail server requires that a PIN be enabled on your phone. You will be unable to send or receive e-mail on your phone without at least a 4 digit PIN code. Alphanumeric passcodes are also acceptable.

Setting a PIN on Windows Mobile
- Click Start -> Settings -> Personal tab
- Click Lock
  - If there is an existing device lock and you wish to change it, enter the device lock password and click Unlock.

  • Select the Prompt if Device Unused for box. Choose a time (between five minutes and one hour) from the drop down list.
  • Click the Password type box. Choose between a Simple PIN and a Strong Alphanumeric password.
  • Enter the password you wish to use. Confirm the password.
  • On the hint tab, enter a word or phrase that will help you to remember the password. A good hint will jog your memory, but should provide no clue to anyone else.

Setting up a Passcode on the iPhone
- Open Settings -> General -> Passcode Lock.
  • Enter the 4 digit passcode you wish to use.
  • Confirm your choice when prompted.
  • Select Require Passcode.
  • Select a time from the list (between 5 minutes and 1 hour).

Setting a PIN on an Android Phone
- Open Settings -> Security -> Set Screen Lock
  • Select PIN
    • Enter the 4 digit passcode you wish to use.
    • Confirm your choice when prompted.

SD Card Encryption

We recommend that any external SD cards holding sensitive data be encrypted. Windows Mobile 6 supports this but it is not enabled by default.

To enable encryption of your SD cards
- Click Start -> Settings -> System tab.
- Click on Encryption.
- Check the Encrypt files when placed on a storage card box.

Please note: Files encrypted in this way cannot be opened by any other device. If the device is hard reset (i.e. back to factory settings) then the encryption keys will be lost and the data on the cards will be irrecoverable.