

USQ ICT Services adopts a position of “Maximum Safe Use” with respect to the usage of Mobile devices by USQ staff, USQ students and members of the public whilst on USQ campuses, and on USQ provided Mobile devices everywhere.

Definitions

A **Mobile device** is any portable device that can connect to the Internet and/or store electronic data. Examples of Mobile devices include; mobile phones, smart phones, PDAs, laptop/notebook/tablet computers, wireless enabled devices, e-book readers, portable music players or any portable device capable of storing electronic data (USB drives/sticks).

Data means anything that is processed, analysed, interpreted, organised, classified or communicated in order to serve a useful purpose, present facts or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form. It is important to protect all data wherever it is stored by ensuring it is secure and backed up, and to protect all data when in transit electronically or physically.

Mobile Device Security Recommendations

By their very nature, mobile devices are more prone to loss and theft than fixed devices and therefore appropriate security precautions should be considered.

- Physical security is a major concern for mobile devices, which tend to be small and easily lost, stolen or misplaced. Do not leave mobile devices unattended in locations where they could be easily stolen or misplaced.
- Users should ensure that the mobile devices security features (if available) are enabled and activated, including unlock codes/passwords, device encryption and remote wipe capability.
- An appropriate risk assessment of the impact of data loss should be undertaken before USQ data is stored on a mobile device.

Wireless Networks

Wireless networks and communications are intrinsically less secure and wireless communications can be easily intercepted.

- Connections of mobile devices to access private or protected data should only be through VPN connections to ensure encryption and safety of data while it is being transferred.
- Connect only to trusted access points. Be careful of sites with WiFi such as airport lounges and hotel lobbies. Multiple un-trusted users in this environment allow an opportunity for criminals to intercept your communication.

Data Storage

Control what data is stored on the device. Do not store unnecessary or sensitive data.

- Unnecessary storage of USQ data on mobile devices is discouraged. An appropriate risk assessment of the impact of data loss should be undertaken before USQ data is stored on a mobile device. Unnecessarily storing sensitive data on a mobile device increases the potential consequences in the case of loss.
- Sensitive data should be encrypted if stored on a mobile device. This will help protect the data if the device is lost or stolen.
- When using a laptop, it is important to back up data and store this additional copy in another place, i.e. on a memory stick in case your mobile device is lost or damaged.
- Consider using multiple backup mechanisms and if you travel, have a portable backup device that you can take with you.

Email

Significant amounts of e-mail are generated and transmitted, over the public Internet

- E-mail may include the transmission of corporate records, contracts, financial records, strategic plans and personal remarks.
- Attachments may carry confidential data and are also a security concern.
- Access to e-mail should be protected.

Virus control

Use antivirus software and a personal firewall where possible

- Mobile devices can be just as susceptible to viruses as desktop computers. Industry analysts expect viruses, Trojans, spam, and all manner of scams to grow as the mobile device market grows. A number of vendors offer antivirus and anti-spam solutions.

Disposal

Data can remain on devices until it is securely removed.

- When ready to dispose of the device, be sure to have all sensitive data removed correctly. Simple deletion of data may not remove it permanently from the device.
- Follow USQ's policy for disposing of computer equipment.

More Information

- Please visit [ICT Services information security site](#)