Procedure

Use of mobile devices procedure

Version: 2.5 | **Version effective**: 25/11/2024

Audience

Department wide

Purpose

This procedure sets the requirements for the Department of Education's (department's) use of mobile devices and personally-owned mobile devices.

Overview

The procedure, along with the Use of ICT systems procedure, supports the Information and communication technology (ICT) policy (DoE employees only) to maintain the security and integrity of the department's information, records and systems while providing employees with access to the department's information on mobile devices.

Employees, managers, directors and principals or above must understand their responsibilities when using or approving the use of departmentally owned or personal mobile devices. This procedure also includes the principals' management of their students' use of personal mobile devices within schools.

Departmentally funded mobile devices, voice, email and data access are provided to employees for officially approved departmental business with limited personal use.

Under certain conditions, the department allows employees to access its ICT applications, systems and networks by using their personally-owned devices. Where ICT services, facilities and devices are provided or made available for use by the department, employees must use them appropriately. Information about the connection services that are available within the regional and central offices can be found in Services Catalogue Online (KBA0016001) (DoE employees only).

The department does not accept liability for any personally-owned mobile devices that are lost or damaged as a result of using the department's ICT facilities, systems, network or services, nor is the department responsible for any repairs or maintenance. The department does not provide any technical or software support to an employee's personally-owned device, except when the employee is accessing departmental applications.

It is mandatory that all departmentally owned school and corporate mobile devices (smart phones, tablets) are enrolled in Intune or another school-owned Mobile Device Management (MDM) platform (see Services Catalogue

Online Intune MDM KBA0025739 (schools) and KBA0034755 (regional and central offices) (DoE employees only) to ensure all mobile devices are administered in accordance with departmental policies.

Responsibilities

Departmental mobile devices and their services

Employees

- ensure they comply with the Departmental mobile devices and services - Conditions of use
- ensure their use can withstand public scrutiny and/or disclosure of usage with respect to limited personal use (including short message services (SMS), multi-media messaging services (MMS), data use and phone calls)
- ensure departmental information with an information security classification (DoE employees only) of PROTECTED is not accessed through or stored within the mobile device
- use a passcode/password, face recognition and/or fingerprint on a mobile device and, where possible, install, run and update anti-virus software
- ensure their mobile device has an ICT asset identification mark or label
- make available the mobile device for regular audit activities which requires the mobile device to be sighted and checked such as for annual stocktakes
- understand that, where abnormal usage is detected, the department reserves the right to limit or temporarily suspend their service at its discretion
- use the mobile device and service during vacation periods under the existing conditions of use ensuring there is a legitimate business requirement, and where necessary, allowing a backfill to the role to use the mobile device and its service
- ensure they protect the mobile device and not leave in a place viewable by the public
- when travelling overseas, initial approval must be sought to take a departmental device overseas by their director, principal or above in addition to applying (via Services Catalogue Online (KBA0010976) (DoE employees only)), for an International Roaming Casual Voice and/or Data pack for their mobile service
- ensure they comply with Transport Operations (Road Use Management—Road Rules) Regulation 2009 (Qld), and not use their departmental mobile phone while a vehicle is either moving or is stationary but not parked
- understand that they will be liable for fines incurred if they operate a mobile device in a motor vehicle in an unlawful manner
- understand that the department will not release a departmental mobile service (except under exceptional circumstances) to an employee leaving Queensland Government, to their new employer or to another Queensland Government department
- return the mobile device upon leaving the department after removing any personal information or photos and ensuring any departmental information is saved onto the department's network, file storage, repository or authorised recordkeeping system

- contact the IT Service Centre on 1800 680 445 if their mobile device is lost or stolen to organise barring of the service (all stolen mobile devices should be reported to the police).

Managers, directors, principals or above

- evaluate employee's work-related requirements for a departmental mobile device including the provisioning of technology and devices to assist employees and/or students of all abilities
- approve the purchase of a mobile device from an approved reseller such as those under the supplier list (DoE employees only)
- ensure all departmental SIM cards are requested through Services Catalogue Online (KBA0016972) (DoE employees only)
- ensure the mobile devices' model, serial number and International Mobile Equipment Identity (IMEI) of all mobile devices are recorded in an asset register according to the ICT asset management procedure
- maintain a local use register if the mobile device is used by a number of employees
- check the activities on the department's mobile devices monthly billing statement and/or internet use report available through the Services Catalogue Online (DoE employees only)
- ensure the recovery of any mobile device and SIM card allocated to an employee who is leaving the department or moving to another agency to avoid liability for costs, and manage as per the ICT asset management procedure
- monitor use according to this procedure and Code of Conduct, taking action where necessary, which could include requesting a reduction of usage or suspension of service
- enhance, retire or replace the mobile device as per the ICT asset management procedure
- request through the Services Catalogue Online (KBA0010751) (DoE employees only) for the porting of a service to a different carrier (e.g. Telstra to Optus or Optus to Telstra)
- understand that the department will not take over a mobile service from another employer other than a mobile service coming from another Queensland Government department, where possible.

Personal mobile devices

Employees

- ensure the use of their personally-owned mobile device meets the requirements of this procedure as well as the Use of ICT systems procedure, Code of Conduct and Standard of Practice
- complete and be up-to-date with all mandatory training (DoE employees only)
- follow any conditions of use when using a personally-owned mobile device to access departmental information, application or online service regardless if the personal mobile device is in place of departmental mobile device or not
- manage the access and use of departmental information in accordance with the level of sensitivity (i.e. information security classification (DoE employees only) of that information
- ensure all departmental information is saved and stored into the department's network, file storage, repository or an authorised recordkeeping system

- accept responsibility for the safeguarding of departmental/school information if stored on their personal mobile device including, not using private email accounts or systems and messaging applications for departmental/school related business
- ensure they meet the department's security requirements enabling the locking of the personal mobile device by the use of a passcode/password, face recognition and/or fingerprint and where possible installing, running and updating anti-virus software
- understand that the department's internal applications e.g. Outlook, OneSchool etc. will work only on operating systems that are no more than two versions behind the latest version available or within three years of the general availability of a new release, whichever occurs earlier
- accept that where their personal mobile device uses an unsupported operating system the department's publicly available mobile applications e.g. Your Passport to Queensland, may not function until the mobile device is upgraded and includes a supported operating system (being no more than three versions behind the latest available version for Apple iOS, and five versions behind the latest available version for Android)
- accept that if the operating system on their personal mobile device is no longer supported by the vendor, the department's support for that version will cease immediately e.g. Windows phone
- ensure all software and other material on their personal mobile device complies with licensing, copyright and any other intellectual property requirements
- ensure their personal mobile device and the taking of photographs is used in a lawful, responsible and ethical manner including compliance to the department's Standard of Practice
- protect their screen when viewing departmental information on their personal mobile device especially when in public
- ensure they no longer have departmental information on their personal mobile device:
  - when the information is no longer required for departmental work purposes
  - before leaving their employment with the department
  - before any exchange of equipment under warranty or for repair, or
  - before disposal of the personal mobile device.
- accept that their manager, director, principal or above may restrict or deny access to the department's network by any personal mobile device used on departmental premises (e.g. schools, central or regional offices) and that access to a restricted ICT service or facility without authorisation, this includes accessing or altering any information stored in, or communicating its information directly or indirectly in anyway, is unlawful under the *Criminal Code Act 1899* (Qld)
- understand that the department may conduct security audits, assessments and scans of any personal mobile device connected or proposing to connect to the department's network if at any time the security of the network is at risk.

Managers, directors, principals or above

- determine and allow, if appropriate, the use of a personal mobile device in place of a departmental device
- understand that the department will not take over a personal mobile service
- monitor use according to this procedure.

Principals

- develop appropriate programs, policies or procedures relating to students' use of personal mobile devices within their school (see Advice for state schools on acceptable use of departmental ICT service, facilities and devices)
- approve student access to the school/department's network where the student's personal mobile device meets security requirements enabling the locking of the personal mobile device by the use of a passcode/password, face recognition and/or fingerprint and where possible installing, running and updating anti-virus software.

Process

There are three processes that assist in managing the use of mobile devices:

1. Departmental mobile devices and their services
2. Employee's personal mobile devices
3. Principals' management of students' personal mobile devices within schools.

1. Departmental mobile devices and their services

The following flowchart outlines the steps required by a manager, director, principal or above to manage a mobile device and their services:

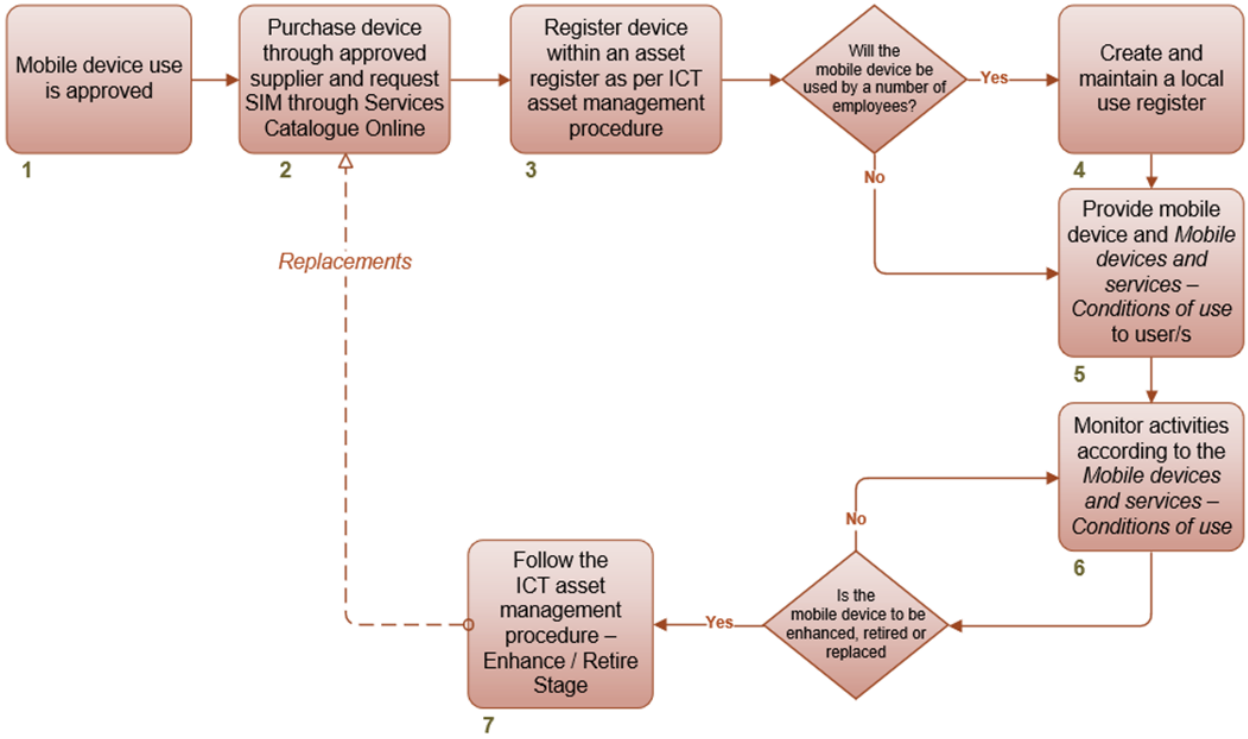

Image 1 Departmental mobile devices and their services flowchart

1. Determine if a mobile device can be provided to an employee based on the requirements of their role to conduct work-related business using a mobile device, or with the assistance of mobile technology. They should also consider technology and devices to assist employee or students of all abilities, for example a

dedicated laptop for teacher aides acting as a scribe. Assistance in the management of these mobile devices for schools can be found within Services Catalogue Online (DoE employees only) under 'Mobile Device Management (MDM)' (see Intune MDM KBA0025739 (schools) and KBA0034755 (regional and central offices)).

2. Once approved, purchase the mobile device from an approved supplier and separately request the SIM through Services Catalogue Online (KBA0016972) (DoE employees only).
3. Once the mobile device is received, ensure it is registered as an ICT asset within the SAP asset register (central and regional offices) or the OneSchool Agresso asset register (schools) as per the ICT asset management procedure. Mobile devices are marked carefully by stamping, engraving, stencilling or other appropriate method subject to any limitations within the manufacturer's warranty. Do not write over or cover any serial numbers or logos.
4. If the mobile device is being shared by employees, ensure a local use register is created and maintained to track the mobile device's location.
5. Ensure the employee/s is provided with a copy of the Departmental mobile devices and services - Conditions of use when receiving the device. Advise the employee/s that their use will be monitored in accordance with the Departmental mobile devices and services - Conditions of use, which addresses:
   - integrity and impartiality
   - accountability and transparency including the monitoring of use, use when travelling overseas and use during leave
   - health and safety
   - security including lost or stolen mobile devices
   - contractual requirements including changes to a service.
6. Monitor use activities as per the Departmental mobile devices and services - Conditions of use.
7. Ensure the ICT asset management procedure is followed when a change to the mobile device is required such as:
   - when an employee is leaving the school/department the mobile device and SIM card are returned
   - when an employee is on extended leave and the mobile device is transferred to their temporary replacement
   - the mobile device and service is transferred only if the situation meets the requirements within the Departmental mobile devices and services - Conditions of use
   - the re-commencement of this process for replacement mobile devices.

2. Employee's personal mobile devices

The following diagram provides an overview of the steps required:

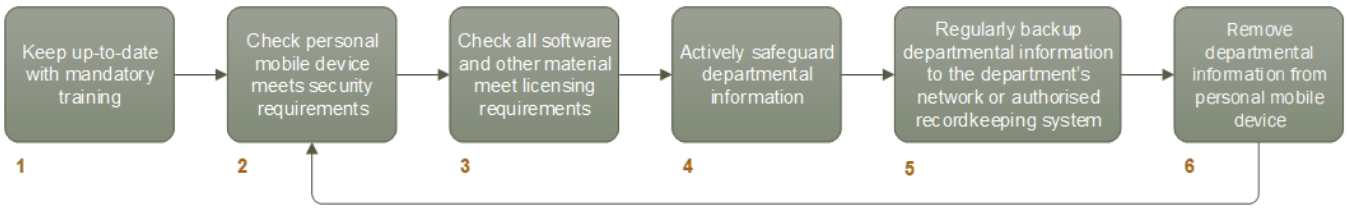

Image 2 Employee's personal mobile devices diagram

Employees need to understand their responsibilities outlined above and continually manage their personal mobile device as follows:

1. Check that they are up-to-date with all their mandatory training.
2. Check that the device meets the department's security requirements at a minimum by enabling the locking of the personal mobile device, such as a passcode/password, face recognition and/or fingerprint, and where possible install and manage their own anti-virus software.
3. Check that all software, and other material on the personal mobile device has been acquired lawfully and complies with licensing, copyright and any other intellectual property requirements. Follow departmental procedures, school policies (if applicable), rules on their use and any warnings provided.
4. Actively safeguard information by using the personal mobile device in secure areas, managing the department's information according to its information security classification (DoE employees only) using the device in a lawful responsible and ethical manner. This includes not using personal email accounts or systems (such as Gmail, Hotmail or similar) and other applications (such as Facebook Messenger, Snapchat, Tiktok and WhatsApp) for departmental or school related business.
5. Regularly backup departmental information on the personal mobile device to the department's network, file storage, repository or authorised recordkeeping system.
6. Remove departmental information from the personal mobile device when not required, before leaving the department, before any exchange of equipment under warranty or for repair (where possible) or before disposal of the mobile device.

3. Principals' management of students' personal mobile devices within schools

Principals will undertake the following steps on a continual basis:

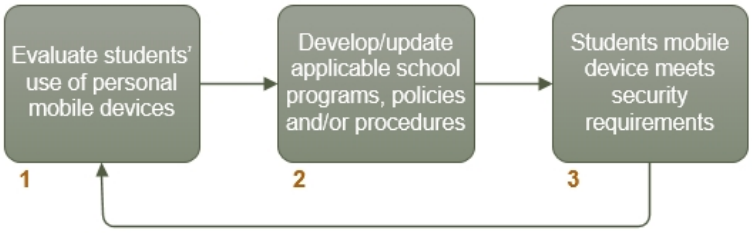

Image 3 Management of students' personal mobile devices within schools diagram

1. Evaluate the benefits and risks of allowing students' personal mobile devices to access the school/department's services or network, and determine under what circumstance if any, they can or cannot use their personal mobile device in school.

2. Develop and maintain appropriate programs, policies or procedures related to the use of students' personal mobile device (if applicable) within their school with the assistance of the Advice for state schools on acceptable use of departmental ICT services, facilities and devices.
3. If a student's personal mobile device connection is to be allowed, determine an appropriate process to validate whether the student's personal mobile device meets security requirements at a minimum enabling the locking of the mobile device by the use of a passcode/password, face recognition and/or fingerprint and where possible the student's parent, guardian or carer has installed and manages an anti-virus software.

Definitions

Term	Definition
Authorised recordkeeping system	A system used to manage and provide access to records over time using a rigorous set of business rules intended to preserve the context, authenticity and integrity of the records. For corporate users, the department's authorised recordkeeping system is HP Record Manager (HPRM). For further information see the Information asset and recordkeeping procedure.
Employee	Any permanent, temporary, seconded, casual or contracted staff member, contractors and consultants or other person who provides services on a paid basis to the department that are required to comply with the department's policies and procedures. Within schools this includes principals, deputy principals, heads of department, heads of curriculums, guidance officers, teachers and other school staff. Volunteers depending on the engagement may not be considered employees but should have regard for this procedure.
ICT asset	ICT hardware, software, systems and services including voice, video and unified communication such as telephony and collaboration systems that are used in the department to process, store or transmit information such as computers, telephone systems, closed circuit television (CCTV) and video surveillance systems, servers, switches, wireless network equipment, cabinets, scanners multifunctional printers, mobile phones, laptops, iPads, Surface Pros, digital cameras, electronic whiteboards, projectors etc.
Mobile device	A portable computing or communications device with information storage capability that can be used from a non-fixed location. Mobile devices include mobile and smart phones, laptops, notebooks, tablets, personal digital assistants (PDA), eBook readers, game devices, voice recording devices, cameras, USB drives, flash drives, DVDs/CDs or hard disks, and other electronic storage media or hand-held devices that provide retention and mobility of data.
Personal mobile device	A mobile device owned wholly by the individual or employee and not by the department, or whereby the mobile device is being paid for by the individual under an arrangement with the department where at the end of the arrangement the individual will personally own the device.

Legislation

- *Transport Operations (Road Use Management—Road Rules) Regulation 2009* (Qld)
- *Criminal Code Act 1899* (Qld)

Delegations/Authorisations

- Nil

Policies and procedures in this group

- Nil

Supporting information for this procedure

- Departmental mobile devices and services - Conditions of use

Other resources

- Queensland Government's Use of ICT services, facilities and devices
- Information and Communication Technology (ICT) (DoE employees only)
- Code of Conduct for the Queensland public service
- Standard of Practice
- Use of ICT systems procedure
- ICT asset management procedure
- Use of ICT facilities and devices guideline
- Information security classification (DoE employees only)
- Service Catalogue Online (DoE employees only)

Contact

For further information, please contact:

ICT Governance team,
Governance, Risk and Compliance,
Information and Technologies Branch
Email: ICTPolicy@qed.qld.gov.au

Review date

22/05/2023

Superseded versions

Previous seven years shown. Minor version updates not included.

3.0 Use and allocation of departmental funded mobile devices and services

2.0 Use of mobile devices

1.0 Use of mobile devices

1.0 Information Communication and Technology (ICT)

Creative Commons licence