Procedure

Use of mobile devices procedure

Version: 3.0 | **Version effective**: 13/07/2026

Audience

Department-wide

Purpose

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

Overview

The procedure, along with the Use of ICT services, facilities and devices procedure, supports the Information and communication technology (ICT) policy 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. Mobile devices include, but are not limited to, mobile and smart phones, smart watches and wearable devices, laptops, storage drives etc.

Under the Education and Care Services National Law Act 2010 (Vic), State Delivered Kindergarten (SDK) employees and volunteers (including students on placement) must not have a privately-owned device in their possession or under their control when working directly with kindergarten children, except for authorised purposes (refer to the SDK Safe use of digital technologies and online environments policy (DoE employees only)). SDK employees or volunteers authorised to use a privately-owned device and/or to be in the possession or control of a privately-owned device, must not use the privately-owned device to capture, store or transmit an image of a child, whilst the child is being educated or cared for by the SDK.

Employees, managers, principals, directors or above must understand their responsibilities when using or approving the use of departmentally-owned or privately-owned mobile devices. This procedure also includes principals' management of their students' use of privately-owned 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 (DoE employees only) (excluding SDKs).

Under certain conditions the department allows employees to access its ICT applications, systems and networks by using their privately-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 internal connection services

that are available within the regional and central offices can be found in Work from Home/Remote Access options for Corporate staff (DoE employees only) (KBA0016001) on Services Catalogue Online (SCO).

The department does not accept liability for any privately-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 privately-owned device, except when the employee is accessing departmental applications.

Responsibilities

Employees

- comply with the Departmental mobile devices and services - Conditions of use
- use privately-owned mobile devices in compliance with the department's information security requirements while accessing departmental information, applications or services
- use current licensed software and operating systems on privately-owned mobile devices, and apply updates as required
- safeguard the department's information on privately-owned mobile devices by using the department's applications when possible and regularly moving any departmental information back to the department's network, file storage, repository or authorised recordkeeping system.

Managers, principals, directors or above

- assess whether an employee is eligible for a departmental mobile device or service and follow appropriate school or business unit purchase approval processes
- ensure that new mobile devices are registered in the appropriate ICT asset register and, where required, maintain a local use register
- ensure departmental mobile phones and tablets are enrolled in Intune or another Mobile device management (MDM) platform
- provide employees who obtain a departmental mobile device and/or service with the Departmental mobile devices and services - Conditions of use and assist with understanding the requirements
- monitor the use of the department's mobile devices and services and, if necessary, take action on inappropriate use.

Principals

- develop appropriate programs, policies or procedures for managing student's use of privately-owned mobile devices within the school
- approve student's access to the school or department's network and monitor their use to ensure security requirements are met.

Process

A process for management is provided for the following mobile device types:

- departmental mobile devices and services

- privately-owned mobile devices of employees (excluding SDK)
- privately-owned mobile devices of students within schools.

Managing departmental mobile devices and services

The following flowchart outlines the steps required to manage departmental mobile devices and services:

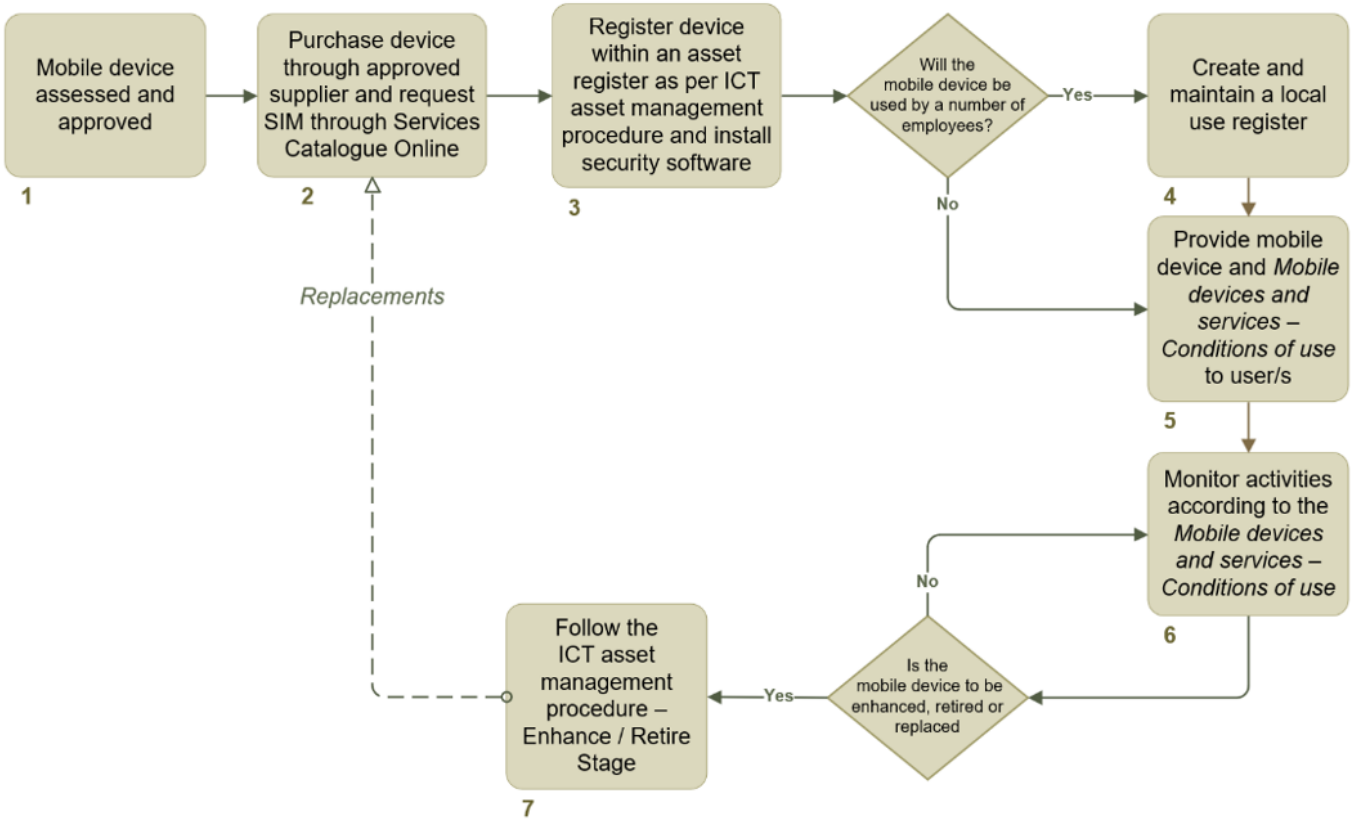

Image 1 Management of departmental mobile devices and services flowchart

1. The manager, principal, director or above will determine if a mobile device or service can be provided to an employee based on the requirements of their role, considering:
   - if the device will be used in SDKs then the Safe use of digital technologies and online environments policy (DoE employees only) must be followed
   - technologies and devices that may assist employees working with students of all abilities, such as a dedicated laptop for a teacher aide acting as a scribe
   - if an employee can use their privately-owned mobile device (excluding SDKs) in place of a departmental device and service, or use their privately-owned mobile device with a departmentally provided SIM
   - ensure all relevant approvals (including financial) are sought.
2. Once approved:
   - eligible school employees can request a Computers for Teachers (CFT) mobile device, CFT mobile broadband SIM card (or eSIM) and, if required, a mobile hotspot through Services Catalogue Online (CFT mobile broadband SIM form). For further information refer to the Computers for Teachers (CFT) Mobile Broadband SIM FAQ (DoE employees only) (KBA0018994)

- all other employees can purchase a departmental mobile device from an approved supplier (DoE employees only). The department's EduPurchasing (DoE employees only) provides an easy way to compare models and prices for mobile devices (excluding Android or ChomeOS devices)
- if required, SIMs can be requested separately through the Mobile service order (DoE employees only) SCO form.

3. Once the mobile device is received, the manager, principal, director or above will:
   - ensure its model, serial number and, where applicable, the International Mobile Equipment Identity (IMEI), are registered as an ICT asset within the SAP (Systems, Applications and Products) asset register (regional and central offices) or the OneSchool Asset Register (schools) as per the ICT asset management procedure
   - ensure the mobile device is carefully marked with its asset number by labelling or other appropriate method subject to any limitations within the manufacturer's warranty. Do not write over or cover any serial numbers or logos
   - enrol departmentally-owned school, regional and central office mobile devices (such as smartphones and tablets) excluding managed operating environment (MOE) laptops, into Intune or another school-owned MDM platform so all mobile devices are administered in accordance with departmental policies. For more information on enrolling mobile devices in Intune:
     - schools can refer to Intune MDM (DoE employees only) (KBA0025739)
     - regional and central offices can refer to Intune for Corporate: Overview (DoE employees only) (KBA0034755)
   - ensure portable storage devices such as USB drives are encrypted and protected with strong password using BitLocker To Go (DoE employees only) (KBA0019296).
4. If the mobile device is being shared by employees, the manager, principal, director or above must create and maintain a register to track who has the mobile device. SDK employees can only share departmentally-owned mobile devices with other SDK employees.
5. The manager, principal, director or above must provide employees with a copy of the Departmental mobile devices and services - Conditions of use when they receive the device and advise them that their use will be monitored in accordance with the 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. The manager, principal, director or above will monitor employee use according to the Departmental mobile devices and services - Conditions of use and the department's Code of Conduct and Standard of Practice:
   - Assess employees' use by reviewing the department's mobile devices monthly billing statement and internet use report available through InfoView as per the Telephone and Billing Information - InfoView FAQ (DoE employees only) (KBA0020835).

- If issues are identified they can be reported via the Log a job to Telecoms (DoE employees only) SCO form.
- Take action where necessary, which could include requesting a reduction of usage or suspension of service.
- Immediately report theft/privacy data breaches in accordance with the Privacy data breach and complaints procedure.

7. When an employee is leaving the department, the manager, principal, director or above must review the requirements for their mobile device and ensure the SIM card and/or mobile device are returned and:
   - if the device is to be retired, written off and replaced follow the ICT asset management procedure (Stage 5: Enhance or retire)
   - if the SIM card is to be cancelled submit a Log a job to Telecoms (DoE employees only) SCO form
   - start this process at step 2 for replacement mobile devices.

Employee's use of their privately-owned mobile devices (excluding SDK) within the department

Employees can use their privately-owned mobiles devices within the department for work purposes except employees within an SDK who must follow Safe use of digital technologies and online environments policy (DoE employees only).

The following flowchart provides an overview of the steps required:

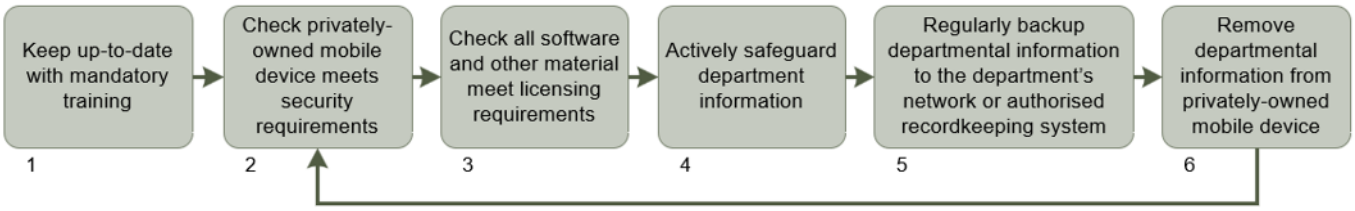

Image 2 Employees' privately-owned mobile devices diagram

Employees need to continually manage their privately-owned mobile device when accessing departmental information, applications or services as follows:

1. Keep up to date with mandatory training.
2. Check that the privately-owned mobile device meets the department's security requirements by:
   - where available, enabling a lock on the device, such as a passcode/password, face recognition and/or fingerprint, and use encryption facilities including USB drives
   - installing and managing anti-virus software where possible and keeping it up to date
   - installing the latest security updates and running the latest supported operating system ensuring they are no more than three versions behind the latest available version for Apple iOS, or five versions behind the latest available version for Android.
3. Check that all software, and other material on their privately-owned mobile device have been acquired lawfully and complies with licensing, copyright and any other intellectual property requirements. Follow relevant departmental procedures, school policies (if applicable) and rules on their use, and any system warnings provided by the software.

4. Actively safeguard information by:
    - checking that no one else can view the screen when using the privately-owned mobile device
    - managing the department's information according to its information security classification (DoE employees only)
    - only accessing restricted ICT services or facilities with authorisation. Accessing, altering or communicating restricted information directly or indirectly in anyway without authorisation, is unlawful under the Criminal Code Act 1899 (Qld)
    - only accessing PROTECTED information through departmentally approved and secured applications or services as they meet relevant security controls and prevent local insecure storage
    - taking photos in a lawful, responsible and ethical manner in compliance with the department's Standard of Practice
    - keeping any departmental or school information temporarily stored on privately-owned devices to a minimum and only if necessary for related work
    - not using personal accounts in systems (such as Gmail, Outlook or similar) and other applications (such as Facebook Messenger, Snapchat, TikTok and WhatsApp) for departmental or school related business:
        - o any personal information (including photos) obtained as an employee must not be use or disclosed within personal accounts
        - o personal email accounts may only be used for multifactor authentication, where required, or in emergency situations when the department systems are down
    - not forwarding or uploading personal information that has been collected unlawfully to a departmental system (for example, recordings made on a personal phone/dashcam that have not provided the subjects of those conversations with a collection notice)
    - forwarding any departmental or school email that is sent to a personal email account or system to an appropriate departmental email account within 20 calendar days of receiving it. Any response to the email must come from a departmental email account.
5. Regularly backup departmental information temporarily stored on privately-owned mobile devices to the department's network, file storage, repository or authorised recordkeeping system.
6. Remove departmental information from their privately-owned mobile devices after use and transfer it to an approved authorised recordkeeping system as per the Records management procedure. All departmental information must be removed before leaving the department, exchanging or disposing of the mobile device, or, when possible, before undertaking repair.

Employees must be aware that the department:

- will immediately cease support/advice for any device running an operating system that is no longer supported by the vendor, such as Windows 10
- may conduct security audits, assessments and scans of any privately-owned mobile device connected or proposing to connect to the department's network if at any time the security of the network is at risk such as due to a cyber threat or incident

- managers, principals, directors or above may restrict or deny access to the department's network by any privately-owned mobile devices used on departmental premises (such as schools, regional or central offices).

Principals' management of students' privately-owned mobile devices within schools

The following flowchart outlines the process that principals will follow to manage student's use of privately-owned mobile devices:

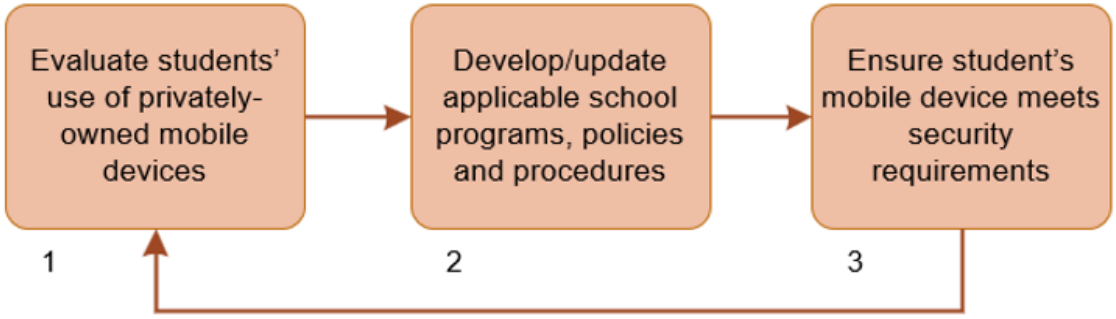

Image 3 Management of students' privately-owned mobile devices within schools diagram

Principals will undertake the following steps:

1. Evaluate the benefits and risks of allowing students' privately-owned mobile devices to access the school or department's services or network, and determine under what circumstance, if any, they can or cannot use their privately-owned mobile device in school.
2. Develop and maintain appropriate programs, policies or procedures related to the use of students' privately-owned mobile devices (if applicable) within their school in line with:
   - Student use of mobile devices procedure that states mobile phones are to be away for the day during school hours and notifications on wearable devices switched off so that phone calls, messages and other notifications cannot be sent or received during school hours, unless an exemption has been permitted under the school's local policy such as for medical, disability and/or wellbeing reasons.
   - Advice for state schools on acceptable use of ICT services, facilities and devices that outlines the controls that need to be considered when allowing students to access the department's network and a template to assist schools in creating an ICT responsible use policy, procedure or guideline.
3. If a student's privately-owned mobile device connection is to be allowed, ensure their privately-owned mobile device meets security requirements, at a minimum by enabling a lock on the mobile device such as a passcode or password, face recognition and/or fingerprint and, where possible, that the student's parent, guardian or carer has installed and manages an anti-virus software. Use of the Department's BYOx link program (DoE employees only) (KBA0031804) is encouraged as it can ensure a base level of security such as the device being secured with a PIN or Password and help facilitate automatic connection to the department's network.

Definitions

Term	Definition
Authorised recordkeeping system	An ICT business system designed to capture, manage and provide access to records through time, that is intended to preserve the context, authenticity and integrity of the records. Authorisation is provided by a principal, an executive director or above, ensuring compliance with recordkeeping requirements such as the *Public Records Act 2023* (Qld) and Queensland Government's Records governance policy. Examples of approved recordkeeping systems include Content Manager for regional and central offices, the OneSchool (DoE employees only) suite of applications for schools or suitable secure file location on school servers. ICT business systems that do not qualify as an authorised recordkeeping system include email systems (such as Outlook), OneDrive or Teams. Further information can be found in Records management (DoE employees only) OnePortal page and Records management 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, portable devices, digital cameras, electronic whiteboards, projectors etc.
ICT devices	Electronic or digital devices/equipment designed for a particular communication and/or function, including but not limited to computers, mobile devices, television sets, interactive panels and boards, gaming/esports (DoE employees only) consoles and equipment, augmented or virtual reality equipment, AV/media streaming and storage devices, and digital or analogue records such as DVD and video, photocopiers/printers and other imaging equipment.
ICT facilities	An electronic capability designed for a particular communication and/or function, which includes but is not limited to electronic networks, online environment, internet, extranet, email, instant messaging, artificial intelligence (AI) including generative AI, webmail, fee-based web services and social media.

Term	Definition
ICT services	Telecommunications services that carry voice and/or data and includes applications, hosting, storage, and cloud-based services etc.
Information	Information is any data that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose, present fact or represent knowledge in any medium or form. This includes presentation in digital, print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form. Information may also form a record or an information asset if it meets certain criteria.
Mobile device	A portable digital computing or communications device capable of storing information that can be used from a non-fixed location to connect to the department's ICT services, facilities and devices. Mobile devices include, but are not limited to, mobile and smart phones, smart watches and wearable devices, 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 information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: • whether the information or opinion is true or not, and • whether the information or opinion is recorded in a material form or not.
Privately-owned 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 privately own the device. Also known as a personal electronic device. It also includes bring your own device (BYOx) initiative.

Legislation

- *Education and Care Services National Law Act 2010* (Vic)
- *Criminal Code Act 1899* (Qld)
- *Information Privacy Act 2009* (Qld)
- Transport Operations (Road Use Management—Road Rules) Regulation 2009 (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

- Code of Conduct for the Queensland public service and Standard of Practice
- Records management procedure
- Information security classification (DoE employees only)
- Privacy data breach and complaints procedure
- Public Service Commission's Private email use policy
- Queensland Government's Use of ICT services, facilities and devices
- Safe use of digital technologies and online environments policy (DoE employees only)
- Services Catalogue Online (DoE employees only)
- Student use of mobile devices procedure
- Use of ICT facilities and devices guideline (DoE employees only)

Contact

For further information, please contact:

ICT Governance team,
Governance Risk and Compliance,
Digital Innovation Division
Email: ictpolicy@qed.qld.gov.au

Review date

13/07/2029

Superseded versions

Previous seven years shown. Minor version updates not included.

2.0 Use of mobile devices

1.0 Use of mobile devices

Creative Commons licence

Attribution CC BY

Refer to the Creative Commons Australia site for further information