DURHAM CATHOLIC DISTRICT SCHOOL BOARD
Learning and Living in Faith

ADMINISTRATIVE PROCEDURE – 431-2

Board Issued Mobile Devices

Area:	Operations
Policy Reference:	Acceptable Use of Information and Communications Technology (PO431)
Approved:	December 8, 2014
Revised:	February 24, 2023; February 14, 2024

1. Purpose

The purpose of this administrative procedure is to define standards, procedures, accountability, restrictions for end users who have legitimate business requirements to access Durham Catholic District School Board (the "Board")'s data from a mobile device.

2. Definitions

Nil

3. Procedures

3.1 Device Allocation

3.1.1 Where necessitated by job requirements, Board staff will be provided with appropriate devices and technology to support their work. The discretion as to whether a job requirement includes access to a mobile device is exercised by a department manager or superintendent and approved by the Chief Information Officer ("CIO"). In all cases, the model/type of device will be selected by Information and Communication Technology Department (ICT).

3.1.2 All employees who have been allotted a mobile device (e.g., smartphones, laptops, iPads, Chromebooks) must complete the electronic Mobile Devices Staff Sign-off Form at https://dcdsb.ca/MobileDevice (complete one form per mobile device issued).

3.1.3 Upgrading of mobile devices will be at the discretion of ICT.

3.1.4 Employees who are on a leave of absence from the Board (e.g., short/long term disability, maternity leave) for a period of four (4) weeks to two (2) years will be provided with the following options with respect to their Board issued mobile device:

1. Return the Board issued mobile device and pause the plan until such time that the employee returns from leave;
2. Retain the Board issued mobile device with unlimited data, talk and text at the employee's expense; OR
3. Retain the Board issued mobile device with only talk and text at the employee's expense.

3.1.5 When an employee who has been issued a mobile device leaves the Board or has a change of position that no longer warrants having the device, their device must be returned to ICT, with no option for retention of the device. In the case where the employee is moving into a new position within the Board that has also been deemed to require a Board issued mobile device, the employee may retain the device with the approval of their supervisor and ICT.

3.1.6 Mobile devices (new and/or previously used) are not available for purchase.

3.2 Costs Associated with Allocated Devices

3.2.1 Monthly usage costs for iPads/tablets/smartphones are covered centrally. Long distance charges and data roaming charges that exceed $10.00 will be billed back to the user unless they are work-related and approved by a Superintendent, Director or designate.

3.2.2 Long distance charges and data roaming charges will be reimbursed for employees using their personal devices for emergency purposes while performing duties on behalf of the Board. These charges must be approved by their immediate supervisor prior to reimbursement.

3.2.3 Employees that are provided Board-issued loaner phones are responsible for non-emergency, long distance and data roaming charges, unless approved by a Superintendent, Director or designate.

3.2.4 When travelling near or outside the Canadian border roaming charges may apply. Consult with ICT prior to travelling outside Canada for "roam like home" rates.

3.2.5 All iPads and iPhones will be supplied with a protective case to reduce the potential for damage.

3.2.6 All users are expected to ensure that Board-issued mobile devices are maintained securely. In the event of a damaged, lost or stolen mobile device it is incumbent on the user to report this to ICT immediately (within 24 hours) by submitting the Property Loss Incident Report (Form AF431-2A) and returning

any damaged mobile devices to ICT. Where it is determined that the damage or loss is a direct result of user negligence, the user may be charged for the costs associated for replacement or repair (whichever is less), or a lesser model may be supplied centrally.

3.2.7 ICT will assume financial responsibility for replacing devices that are reported stolen, provided that a police report is included with the accompanying Property Loss Incident Report (Form AF431-2A).

3.2.8 Users acknowledge and accept that any apps purchased using Board funds remain the property of the Board.

3.2.9 The Board reserves the right to prohibit the downloading and usage of specific apps at any given time.

3.3 Use of Mobile Devices in School Classrooms or Board Work Sites

3.3.1 Use of mobile devices in school classrooms are permitted subject to the conditions set out in the Acceptable use of Information and Communications Technology Policy (PO431) and Administrative Procedure (AP431-1), Data Access and Management Policy (PO427) and Administrative Procedure (AP427-1).

3.3.2 Except in the case of an emergency, staff are expected to refrain from using mobile devices for personal business during instructional time or the regular workday, outside of scheduled breaks and lunch time.

3.3.3 Board-issued mobile device data cannot be stored on freemium cloud-based systems such as Google Drive, Dropbox, etc. Board data must not be stored on personal devices.

3.4 Driving While Possessing Wireless Devices

3.4.1 Employees must not use mobile devices handheld while driving. This is a violation of the law and prohibited conduct for which they may be personally liable.

3.5 Device Support

3.5.1 ICT staff will only support the device at the connectivity and Operating System level. Support for individual apps is outside of the scope of the support structure.

3.5.2 ICT will assist the user in moving Board contacts, email, calendar and data from an old device to a replacement device.

3.5.3 ICT has established a “depot service” procedure, whereby an individual may drop off their device for service, and ICT may provide a loaner unit until the

original unit is repaired or replaced. The SIM card will be swapped to enable the same number to maintain functionality. The “depot service” may be assumed by the servicing dealer, at the Board’s option. Staff will create a HelpDesk ticket to make an appointment.

3.6 Device Management

3.6.1 ICT will manage a standard configuration and suite of applications on all Board-owned mobile devices. ICT will also manage the configuration of any Board-owned mobile device, and potentially wipe it, track it, or clean remotely if it goes missing.

3.6.2 Connectivity of all mobile devices will be centrally managed by the Board’s ICT department and will utilize authentication and strong encryption measures. Although ICT is not able to directly manage external devices, such as home computers which may require connectivity to the Board’s network, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges to protect the Board’s infrastructure. Any violations to the policy will be reported to the CIO and their senior management representative.

3.6.3 Purchasing, repairing, and replacing of Board-owned mobile devices must be processed through the Board’s ICT department. Staff shall not purchase or repair a device through any other means and will not be reimbursed by the Board if they choose to bypass the Board’s procurement process.

3.6.4 The addition of new hardware, software and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of the ICT department.

3.6.5 Virtual Private Network (VPN) will be provided to users as required to access certain applications remotely.

3.7 Security

3.7.1 All mobile devices must be protected by a strong password in accordance with the direction given by the Chief Information Officer.

3.7.2 Employees must not disclose their passwords or passcodes to anyone.

3.7.3 Any board-owned mobile device that is being used to store Board’s data must adhere to the authentication requirements of Board’s ICT department.

3.7.4 ICT will manage Board information and communication technology systems centrally using technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Board’s overarching

Acceptable Use of Information and Communication Technology Administrative Procedure (AP431-1).

3.7.5 All data stored in the Mobile Device will be erased permanently by ICT if the device is being replaced or is no longer required. Staff are encouraged to use the Board's OneDrive for the storage of Board data.

3.7.6 In the event of a lost or stolen mobile device it is incumbent on the user to report this to ICT immediately by submitting the Property Loss Incident Report (Form AF431-2A) (within 24 hours). The device will be remotely wiped of all data and locked to prevent access by anyone other than ICT. If the device is recovered, it can be submitted to ICT for re-provisioning.

3.8 Protection of Privacy

3.8.1 Individuals, including students, have a reasonable expectation of privacy. All mobile device users must be mindful of privacy expectations, and therefore, must refrain from:

- use of mobile devices in washrooms;
- taking pictures of individuals without consent. The consent of the parent/guardian is required for all students under the age of 18;
- posting of a person's image(s) on the internet or in hard copy;
- emailing pictures and/or recordings of individuals without consent;
- sending inappropriate text messages, emails or images;
- compromising personal and/or school safety (e.g., bullying);
- any other situation deemed by school administration where school security, safety, individual privacy or academic integrity is compromised.

NOTE: The above is not an exhaustive list.

4. Sources

4.1 Education Act, RSO 1990, c. E.2
4.2 Bill 118, Countering Distracted Driving and Promoting Green Transportation Act, 2009
4.3 Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

5. Appendices

5.1 Property Loss Incident Report (Form AF431-2A)

6. Related Policies and Administrative Procedures

6.1 Acceptable Use of Information and Communications Technology Policy (PO431)
6.2 Acceptable Use of Information and Communications Technology Administrative Procedure (AP431-1)

6.3 Data Access and Management Policy (PO427)
6.4 Data Access and Management Administrative Procedure (AP427-1)
6.5 Freedom of Information and Protection of Privacy Policy (PO201)
6.6 Code of Conduct Policy (PO610)
6.7 Code of Conduct Administrative Procedure (AP610-1)

DURHAM CATHOLIC DISTRICT SCHOOL BOARD
Learning and Living in Faith

Property Loss Incident Report

Report Date:

School/Department:

Contact Name:

Principal's Signature:

Date of Incident:

Time of Incident:

Police Contacted: Y N

If Yes, Date Reported:

Investigating Officer:

Badge #:

Police Report #:

Type of Incident: Theft Vandalism Accident Fire Other:

Who witnessed/discovered the incident:

When was the incident discovered:

Were there any signs of forced entry: Y N

What were they:

Were the items in a secure/locked area: Y N
If yes, how were they secured:

Damages (List all damages to property and/or equipment providing as much detail as possible):

Approximate Cost:

Stolen Items (Describe equipment and/or materials including manufacturer, model and serial numbers. Attach proof of ownership for these items either in the form of original PO or Inventory Control Record):

Approximate Cost:

All sections must be completed in full. Incomplete forms will be returned to originator for proper completion. Our insurance carrier requires full documentation in order to process claims. Proof of ownership for the items being reported stolen, lost or damaged are required as supporting documentation. A copy of the original purchase order must be submitted within 30 days of submission of this form to the Purchasing Department, in compliance with Board Policy.

Note: Please attach any extra notes providing details about the incident to this form at the time of submission.

Form Number: AF431-2A
Related Procedure(s): AP431-2 Board Issued Mobile Devices Administrative Procedure