Use of Technology
Policy 224, 2025

The following was approved by the Chief Administrative Officer (CAO) as an Administrative Policy on **Month day, 2024.**

PURPOSE

This policy establishes requirements, conditions, and terms of use for District of Lake Country ("District") cell phones, devices and technology.

POLICY

1. GENERAL

1.1 Definitions:

Equipment means a computer, tablet or cell phone provided by the District.
Technology includes internet, hardware, software, email communication, instant messaging, voice chat, business applications, data, the network and services provided by the District.

1.2 In the event of EOC activation, the CAO may authorize temporary exceptions to this policy.

2. INFORMATION TECHNOLOGY (IT) DEPARTMENT RESPONSIBLITIES

2.1 The Information Technology (IT) Department is responsible for:

(a) the procurement of **Equipment** and **Technology** for District business applications
(b) authorizing all software purchases
(c) maintaining an inventory of District owned **Equipment**;
(d) the management and use of the District's Mobile Device Management system
(e) Tracking lost or stolen **Equipment**
(f) Remotely wiping lost or stolen **Equipment** where required
(g) Resetting device PIN or passwords
(h) following industry standard practices regarding virus protection, firewall security and anti-spam
(i) enabling authentication and encryption tools
(j) adhering to the terms of all software licence agreements to which the District is a party
(k) providing best-effort to support apps required to conduct District business

2.2 IT is not responsible for providing support for devices outside of the manufacturer's specified support period.

3. CELL PHONES

3.1 All Directors and Managers are required to carry and use a cell phone for job-related communication.

3.2 Department Directors are responsible for identifying Exempt and Union positions within their department that are required to have a cell phone for job-related communication.

3.3 Generally, a cell phone is required where:
- (a) it is deemed necessary for safety purposes
- (b) there is a need for "field to office" communication
- (c) alternative communications methods are not available
- (d) it is required for responding in times of emergency
- (e) it is deemed necessary in order to fulfill job-related responsibilities

3.4 Employees required to carry a cell phone may choose:
- (a) a District Owned Device, or
- (b) Bring Your Own Device (BYOD)

3.5 District Owned Devices:
- (a) Are upgraded per the District's standard **Technology** lifecycle plan
- (b) will be managed under the IT Department's Mobile Device Management system
- (c) may be used for personal use not exceeding $5.00 above the current District payment plan; overages shall be reimbursed by the user to the District

3.6 BYOD
- (a) must meet minimum system requirements
- (b) are not managed under the IT Department's Mobile Device Management system
- (c) may connect to the District's Staff Wifi
- (d) may connect to apps and services used and maintained by the District to conduct business

3.7 Summer Students and Lake Country Fire Department (LCFD)
- (a) Summer students and LCFD Paid-on-Call (POC) Members are not eligible for a District Owned Device
- (b) Summer Students identified as requiring a cell phone will be reimbursed in accordance with Travel and Expense Policy 225, 2025.
- (c) LCFD POC Members and LCFD Union Employees required to carry a cell phone, as identified by the Fire Chief will be reimbursed in accordance with Travel and Expense Policy 225, 2025.

3.8 While driving a District vehicle to perform job-related duties, Employees:
- (a) must not:
  - (i) operate or hold cell phones or other electronic devices
  - (ii) send or read emails and/or texts on cell phones
  - (iii) manually program or adjust GPS systems, whether built into the vehicle or not
- (b) may use cell phones:
  - (i) for hands-free incoming or outgoing calls
  - (ii) for GPS when pre-programmed and voice activated
  - (iii) if the vehicle is legally parked and is not impeding traffic
- (c) Notwithstanding items 3.8 (a):
  - (i) LCFD Fire Department Employees are exempt where required to make calls in the performance of their duties
  - (ii) Drivers with a 'Learners' or 'Novice' designation are prohibited from using hand-free communication devices while driving

4. INTERNET AND NETWORK ACCESS

4.1 **Equipment** provided by the District will have internet access at District facilities or where District Wi-Fi is available.

4.2 The District is not responsible for providing internet access outside of District facilities.

4.3 Access to the District's network is granted by the IT Department.

4.4 Personal devices are only permitted to be connected to the DLC-Staff network.

5. PERSONAL USE

5.1 Use of **Equipment** and **Technology** is primarily for business purposes and should be limited to job related duties. Limited personal use is acceptable as long as:

(a) use does not affect work performance or normal business activities
(b) use does not directly or indirectly interfere with **Technology**
(c) use does not compromise the security or reputation of the District
(d) personal files are kept separate from District files
(e) additional costs on District Owned Devices, resulting from personal usage, do not exceed the District's monthly cell use payment plan

6. DAMAGED EQUIPMENT

6.1 Where a District Owned Device is damaged the District is responsible for repairs or replacement.

6.2 Where a personal or a BYOD is damaged the user is responsible for repairs or replacement.

6.3 Where **Equipment** is damaged while being used for District purposes, the District is responsible for repairs and replacement.

7. APPLICATIONS ("apps")

7.1 The District is not responsible for the download, installation, storage or support of apps outside of those required for District purposes.

7.2 Users must ensure any third-party apps adhere to all applicable District policies, bylaws or legislation.

8. INFORMATION STORAGE

8.1 All District information is to be stored on the District's systems.

8.2 Unless authorized by the IT Department, District information shall not:

(a) be stored on the local PC
(b) be saved on non-District systems or servers
(c) be saved on removable drives
(d) be forwarded to personal emails or storage locations

9. ACCOUNTABILITY AND PRIVACY

(a) Users are responsible for all activities conducted under their assigned District user IDs and email addresses
(b) There is no expectation of privacy for work-related information created, stored, or transmitted on District-owned systems, devices, or accounts; limited privacy may apply to personal information on personally-owned devices used for work purposes
(c) The District reserves the right to monitor activities and remotely wipe **Equipment** where required
(d) Lost or stolen **Technology** must be reported to the IT Department as soon as is practical

10. CARE AND SECURITY

(a) All cell phones must have a protective cover or case
(b) **Equipment** must have auto-lock feature set to fifteen minutes or less
(c) **Equipment** must have a password or passcode, as determined by the IT department
(d) Confidential data, authentication credentials, PINs and passwords must be protected and not shared with any other party
(e) Devices must remain in a user's custody
(f) Reasonable measures must be taken to safeguard the physical protection of **Equipment** and devices

11. EMAIL AND NETWORK SAFETY

(a) Suspicious emails or attachments are not to be opened
(b) Unauthorized activity or where the security of a device has been compromised must be reported to the IT Department immediately
(c) Overloading networks with excessive data or wasting the District's **Technology** is not permitted

12. SOFTWARE USE AND LICENSING

(a) The use of unlicensed software within the District must be reported to the IT Department as soon as is practical
(b) Software must only be used in accordance with its licence agreement

13. ACCEPTABLE USE AND CONDUCT

(a) Users of District **Equipment** and **Technology** will not engage in unauthorized or illegal activity under bylaws, policies, procedures, provincial, federal or international law including copyright and networking laws and regulations.
(b) Users will use acceptable etiquette and language

14. VIOLATIONS

14.1 Violations of this policy will be reviewed on a case-by-case basis and may result in loss of access to **Equipment** and **Technology** and disciplinary action up to and including termination, in accordance with District's policies and procedures.

15. PRIVACY AND FREEDOM OF INFORMATION

15.1 All users of **Equipment** and **Technology** must comply with the Freedom of Information and Protection of Privacy Act (FOIPPA). Personal information must only be collected, used, or disclosed for authorized work purposes. Any loss, theft, or unauthorized access involving personal information must be reported immediately. Any record within the custody or control of the District is subject to disclosure under FIPPA.

16. REPEALS

16.1 The following policies are hereby repealed:

(a) Cellular Device Policy 179, 2020
(b) Computer Purchase Program Policy 156, 2017
(c) IT and Computer Use Policy 14.143
(d) Council Device Policy 210, 2024

17. APPROVALS, AMENDMENTS AND ANNUAL REVIEWS

Date	Approver	Type

Mayor **Corporate Officer**

USER ACKNOWLEDGEMENT

I have read and understand Use of Technology Policy 224, 2025 and acknowledge my responsibility to adhere to the requirements contained herein:

Employee Signature	Director/CFO/CAO Signature
Print Name	Print Name
Date	Date

☐ District Owned Device ☐ BYOD ☐ Summer Student Provision ☐ LCFD/POC Provision

Cell Number: _____