COMMUNITY LIVING DURHAM NORTH

INFORMATION AND COMMUNICATION TECHNOLOGY

Policy No: C-24 (Human Resources)

Effective Date: June 30, 2011
Last Revision:
Last Review: July 17, 2023

Rationale:

To ensure that employees understand what is appropriate and inappropriate in their use of workplace information and communication technology.

To ensure the safeguarding and integrity of all Community Living Durham North computer, communication and information technology.

Policy Statement:

CLDN provides its employees with access to communication and information technology for the sole purpose of furthering the objectives of the agency. The use of this technology must be consistent with provincial and federal law, our Mission, Values and Principles, and with this policy statement.

All equipment, hardware and software issued by CLDN remains the property of CLDN, as does the product of the equipment, hardware and software.

Our information and equipment is a corporate resource of substantial value that must be protected from unauthorized use, modification, destruction or disclosure, whether intentional or inadvertent. Software will be purchased to protect our systems from intruders.

Senior management will develop procedures to clearly articulate for employees those uses that are inappropriate and/or illegal. A monitoring system will also be implemented to ensure compliance with these procedures. Failure to comply will result in disciplinary action up to and including dismissal. Illegal use of the agency's technology will be prosecuted.

Approved by: *Larry Leonard* Date: *June 30, 2011*
for the Board of Directors

COMMUNITY LIVING DURHAM NORTH

INFORMATION AND COMMUNICATION TECHNOLOGY

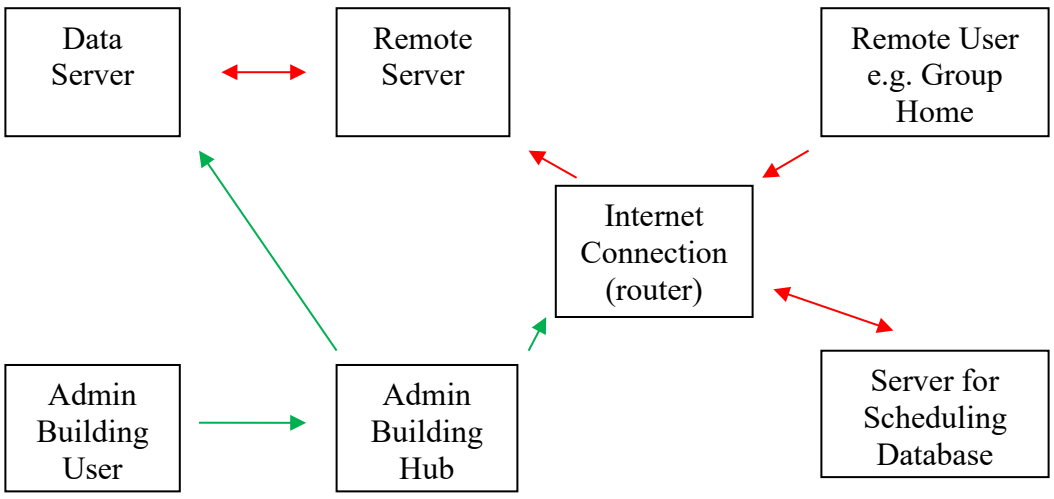
Procedure No: C-24-1 **CLDN's Communication System**	Effective Date: June 30, 2011 Last Revision: December 18, 2013 Last Review: July 17, 2023

- The following diagram will provide the neophyte with a basic sense of how CLDN's communication system is constructed.

  Each User in the Admin Building goes through the Office Hub in order to access the Internet or the main Data Server. The Hub is a portal that enables multiple users to have simultaneous access.

  When our internet connection is lost the User in the office can still go through the Hub and access the main Server.

  Remote Users, in homes or in Resource Centres, are dependent on the internet to get "into the office;" it conducts them to the Remote Server which shares data with the main data server.



Procedure No: C-24-2	Effective Date: June 30, 2011
Security Features	Last Revision: August 9, 2024
	Last Review:

- The internet connection or router is password protected and encrypted. Encryption protects the router from external hackers.

- Both servers and all workstations, including laptops, are secured with (letter/number combination) passwords.

- In the Vanedward main office, the servers and all workstations, are loaded with purchased business versions of leading antivirus software, which is regularly updated. Our antivirus software is also spyware protection. It protects us from pop-up invasions.

- Workstations located in programs and in the 16025 offices, which access the servers remotely, are protected with free versions of the same antivirus software.

- In order to gain access to the server, all remote users must first exercise Multifactor Authentication (MFA) by entering a unique username/password combination and by subsequently entering a secure code from either a soft token (admin staff and managers working remotely) or a hardware token (all program sites).

- If a hardware token is misplaced or lost, then staff will not be able to complete their daily documentation requirements. Therefore, when not in use, all hardware tokens must be stored in the programs' locked Medication Cupboard. Also, the tokens are attached to a painter's stick to prevent people from inadvertently putting them in their pocket and taking them home.

- We have moved our email system from our own server to Microsoft 365; by doing this we avail ourselves of Microsoft's protections against email spam.

- Only properly licensed software will be loaded onto CLDN computer hardware. This function shall be performed by the Manager of IT.

- Users must not install or download any additional software, computer equipment or mobile device onto the CLDN computer system, or onto an individual workstation, without the prior approval of the IT Manager or designate.

- Files received via email are automatically scanned for virus infection. However, users must receive the prior approval of the IT Manager, or designate, before downloading files from the internet and before using flash drives or disks to import them into the CLDN computer environment.

- Every individual user (i.e., all admin staff, managers and team leaders) has a log in name and password, and staff who work in a particular program, or who are trained as replacement staff in that program, share a log in name and password.

- Passwords are confidential (except at shared workstations) and users are responsible for safeguarding their passwords. Assigned passwords cannot be changed by the user; employees must go through the IT Manager if a change is necessary.

- Users are responsible for all transactions made using their passwords.

- Our Manager of IT holds all log in names and passwords and can change or delete any one of them unilaterally. Senior staff (i.e. directors) also have access to this information. The external company from which we purchase occasional computer support has access to the systems level passwords – those on the router and servers. Otherwise, individual passwords or lists of passwords shall not be printed, stored on-line, or given to others. Files containing passwords are password protected and can only be opened by entering the secure password.

- The Manager of IT must be advised, immediately, of all hires and terminations.

- Documents, software and other materials created with agency computers and computer equipment are the property of CLDN. To protect the privacy of supported people, employees and the agency itself, it is important that they not be copied, saved or downloaded onto external media. Remote users – those not based at the main office – lack the capability of doing this; those based at the office are prohibited from doing so without the prior approval of a director. To reinforce the prohibition, personally owned Jump Drives are not permitted in the main office. However, a CLDN Jump Drive can be accessed from the Manager of IT for previously approved purposes.

- It is acknowledged that unauthorized downloads can be effectively performed by attaching documents to an email, one sent perhaps to one's own household PC. This is strictly prohibited and it is one of the reasons that random monitoring of CLDN email traffic is conducted.

- Every program location has its own email account. Knowing its password, it is possible for staff to add the program's account to their personal device. This is not permitted, because at this point sensitive information about supported people has left the workplace, and their privacy has, at least potentially, been violated.

- All employees must complete the mandatory cyber security training provided by CLDN and posted on the Surge Learning platform.

- If CLDN is presented with an order from a law enforcement agency or another legislative authority demanding access to an employee's personal information and usage history contained on CLDN equipment, the agency must comply and we will also advise the employee.

Procedure No: C-24-3	Effective Date: June 30, 2011
Data Storage, Access and Back-up	Last Revision: April 12, 2024
	Last Review:

- All program sites, and all staff physically present at those sites, have log-in access to the agency's remote server where they can create and save documents. They can also save documents on their local C Drive but C Drives should only be used to store working or temporary files that are not part of any person's clinical record, not official CLDN documents, and not meant to be shared outside of the program site. To promote communication across the entire agency, while protecting the security of documents and the privacy of people, formal documents must always be accessed from the agency's Server. No back-up is performed upon individual C Drives.

- Data on the server is "filed" in one or more of the following electronic filing cabinets:

  — Agency Wide
  — Accounting
  — Directors/Managers/Admin
  — Directors/Admin
  — Directors/Managers
  — Directors
  — HumanResources

- This simple "filing system" is the first level of determining access. Directors have access to all seven filing cabinets, Managers to all but Accounting, Directors and HumanResources, etc.

- However, within this system, access can be granted, or removed, on a file-by-file basis, by the IT Manager, or designate. For example, within the "Directors" cabinet, the Executive Director might have a Board folder or individual documents pertaining to the Board to which other directors might not have access.

- The more important examples occur within the Agency Wide cabinet. Here, one of the first level dividers is "People Who Live At." The sub-folders inside that folder are the names of homes and other program locations, which take you in turn to the names of people supported and the documents that pertain to them. Only if you are sitting in front of the computer at Simcoe Street, and you know its name and password, can you access the Simcoe folder and thus gain access to the personal information on the people residing there. This assigning of rights and the continuous monitoring of what people have access to what documents, is a significant component of the IT Manager's day to day job function. It is also key to protecting the privacy of supported people.

- Employees must ensure security precautions are taken when working remotely to guard against:

  - The physical loss or theft of agency information or I.T. equipment/mobile devices;
  - Inappropriate access by non-employees (e.g. family members);
  - Loading and/or transferring data onto home or personal devices;
  - Communicating information through unprotected channels (i.e. wireless security measures must be used);
  - Printing information with inappropriate disposal options (e.g. to the wrong location, leaving printed material on printer without gathering it in a timely manner, or lacking the ability to dispose of material via shredding or recycling).

- It is the responsibility of the IT Manager or designate to ensure that all data is backed up on a nightly basis and that the backup is stored securely in a fireproof locked cabinet. However, backing up our data five times each week quickly seals the fate of a file that is erased or lost if that problem is not detected for a couple of days. For that reason, a back-up is also performed monthly and stored off site at a secure location for a period of three months. When necessary, one of these secondary back-ups can be used to restore lost data.

Procedure No: C-24-4	Effective Date: June 30, 2011
Internet Usage and Passwords	Last Revision: September 1, 2014
	Last Review: July 17, 2023

- CLDN provides internet access to support its operations. Proper use of the internet can enhance opportunities for people receiving service, and can also enhance the effectiveness and the career opportunities of its employees.

- Employees must understand that they do not have an expectation of privacy in their use of CLDN's internet facilities. From time to time and without notice, CLDN randomly monitors internet usage and can record the websites accessed by employees.

- That said, CLDN is a progressive employer and recognizes that, from time to time, employees may wish to briefly "google" some topic out of personal interest or access the internet for another personal reason. This activity is permitted on an exceptional basis only, provided it does not interfere with the employee's job responsibilities or the completion of daily tasks. All such activity must be confined to the employee's lunch hour and/or break times. This privilege may be withdrawn and excessive personal use of the internet will constitute a performance issue subject to discipline up to and including dismissal.

- Most agency computers are blocked from access to social media sites like *Facebook*. However, a few workstations used by senior staff are enabled so that these sites can be accessed for work-related purposes. CLDN has its own *Facebook* page as do many

agencies, including Community Living Ontario, so it is necessary for certain staff to have access.

- Users must not deliberately perform acts that waste computer resources (including network bandwidth, Wi-Fi, disk space, internet usage) or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, uploading or downloading large files, unnecessary printing, streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic.

- Users are not permitted to purchase goods or services for their personal use via CLDN equipment without the express written consent of their Manager.

- CLDN will not be responsible for the misuse of agency internet-related systems. Persons found to have misused the internet will be held accountable for any costs or damages sustained by CLDN, or by a third party, and will be obligated to indemnify the agency or the third party.

- CLDN reserves the right to monitor its use of the internet and to record the websites accessed by employees.

- The illegal use of CLDN's internet shall be reported to police.

- The following activities may be legal but they are not acceptable in CLDN's workplace, and are strictly prohibited:

    - Those unrelated to the agency's mission except as noted above.
    - Those unrelated to job responsibilities, except as noted above.
    - The transmission of threatening, obscene (sexual jokes, etc.) or harassing materials.
    - The unauthorized distribution of agency data and information.
    - Interfering with or disrupting network users, services or equipment.
    - The furtherance of private purposes through marketing or business transactions (i.e. job hunting, on-line banking, etc.).
    - Solicitation for religious or political causes.
    - Representing personal opinions as those of CLDN.
    - Accessing chat lines or dating websites.
    - Accessing, displaying or disseminating material that is sexually explicit, pornographic, racist or otherwise offensive.

  Note that the above list is not intended to be exhaustive. While illegal purposes are easily identified, the employer reserves the right to define what is appropriate and inappropriate in its workplace.

- A user who inadvertently accesses an inappropriate internet site must immediately inform the Manager of IT or any member of the management team.

- Passwords to all CLDN emails and server logins are confidential and users are responsible to safeguard them (i.e. not share or disclose them).

- CLDN will hold the user responsible for all activity that occurs under his/her user name and password. Therefore, the use of another user's account password is strictly prohibited. Users shall immediately report any known or suspected compromise of their passwords to the Manager of Technology.

Procedure No: C-24-5	Effective Date: June 30, 2011
Email Usage	Last Revision: July 17, 2023
	Last Review:

- Every program site and every individual employee has been provided with a CLDN email address, at the agency's expense, to facilitate seamless workplace communication without the necessity of tracking over 300 personal email accounts. Employees are responsible for accessing their CLDN addresses and will be deemed to have received messages sent to them at these addresses.

- The email system is provided by CLDN to assist in the conduct of its business. Messages composed, sent or received on our email system should not be considered secure and are not the private property of any user; they are and will remain the property of CLDN.

- Information in the email system is part of the public record of the agency. Email communication is to be treated in the same way as other kinds of agency correspondence and also held to the same standard.

- CLDN randomly monitors email traffic.

- Notwithstanding the agency's right to monitor all email traffic, employees must treat each other's email correspondence as confidential. That is, employees are not authorized to retrieve or read email messages that are not addressed to them. Exceptions are the Manager of IT and the Director of Admin Services; these employees perform the monitoring function on behalf of the agency. A further exception is employees who share a workstation in a home or Resource Centre. Emails addressed to "Lakeview" may be opened by anyone who works at Lakeview and has been given the name and password for its work station.

- Personal email accounts (e.g. Hotmail or Gmail) are not to be used for any correspondence transmitted across CLDN's mail server.

- As with the internet, the personal use of CLDN's email system is only permitted on an exceptional basis. The use must be brief and it must occur during the employee's lunch hour or break time. This access is a privilege and it will be withdrawn if management considers that it is being abused by an individual employee or by a shared workstation.

- The following uses of the agency's email system are unacceptable and prohibited:

  - Those unrelated to the agency's mission except as noted above.
  - Those unrelated to job responsibilities, except as noted above.
  - Sending messages that are sexually explicit, pornographic, racist or otherwise offensive.
  - Soliciting support for commercial ventures, religious or political causes, outside organizations, etc.
  - Representing personal opinions as those of CLDN.
  - Creating or sending disruptive messages that adversely affect the operation of the computer network and reduce the recipient's ability to perform work.
  - Using email attachments to export data to external media.
  - Sending e-mails that a reasonable person would perceive to be Junk, Spam, or a chain e-mail;
  - Sending e-mails that are forged or that attempt to mislead the recipient as to the sender's identity;
  - Sending e-mails that divulge private and/or confidential information related to CLDN's business, the people it supports, their families and/or its employees, including photos;
  - Sending e-mails that violates any of CLDN's policies including policies related to Professional Conduct or Workplace Harassment;
  - Sending e-mails that are derogatory and disparaging of CLDN or otherwise damaging to its reputation, relationships or interests;
  - Sending e-mails that are designed to damage in any way the recipient's internet system;
  - Any behaviour that constitutes gaming or gambling;

Procedure No: C-24-6	Effective Date:	June 30, 2011
Laptops, Cell Phones and other "Take Home" Equipment	Last Revision:	July 8, 2024
	Last Review:	

- Managers, directors, and administrative staff who need to work in the evenings or on weekends may be furnished with a laptop, cell phone, or similar equipment. Our cell phone plans are basic plans with a fixed cost and are reasonably priced. Employees' personal use of the service does not result in charges exceeding the basic plan cost. Therefore, the personal use of the cellular phone service is not considered a taxable benefit.

- Any charges exceeding the basic plan that are not pre-approved by senior management for business purposes will be billed to the user.

- When this occurs, a signed agreement shall be executed and entered into the employee's Personnel file. It will document that the equipment exists, that it belongs to CLDN, and

that it must be returned to CLDN at the termination of employment, or at any time, upon demand. It will also detail the responsibility of the employee to take care of the equipment and transport it safely, and of the agency to equip it with antivirus and antispyware and to attend to regular maintenance.

- Consistent with the above procedures, the personal use of computer equipment, while at home, is permitted on an exceptional basis, but the same prohibitions also apply around appropriate email and internet usage. Children and other family members must not be granted access.

- As stated above, no agency documents, software and other materials shall be copied, saved or downloaded onto external media. This includes transfers from an agency laptop to a household PC, for which the prior approval of a director is required.

- It is expected that all equipment provided to employees (i.e. car chargers, cases, etc.) will be kept in good repair. When it needs to be replaced because of neglect or loss, the employee may be held accountable for the cost.

Procedure No: C-24-7	Effective Date:	April 2, 2012
The Use of Personal IT Equipment	Last Revision:	July 17, 2023
	Last Review:	

- Some IT equipment likely to engage one's time and attention, like laptops and iPads are not permitted in the workplace without the express permission of the location manager. And, even if express permission is obtained, CLDN (and people supported by CLDN) will not accept responsibility for damage done to this kind of equipment.

- Personal cell phones can be brought into the workplace but must be left in the office; they cannot be kept on the staff's person throughout the shift. This prohibition exists because some people find texting compelling, and also in order to safeguard the privacy of supported people.

- Ringers are to be kept on vibrate or low so as not to become a distraction to other staff or to people who live in the home.

- Communication between employees via text messaging on an agency or personally owned device must be limited to non-identifying matters that maintain the privacy of people supported and employees.

- Staff may use their personal devices to return personal calls or messages during their meal break and their relaxation break(s) only.

- However, it must be noted that staff entitled to only one fifteen-minute break, because they are working a shift of less than five hour's duration, must take one uninterrupted break. Regardless of duration, they cannot have two breaks.

- Employees entitled to 30 minutes of relaxation time may divide their break into two different breaks of 15 minutes each, or of variable length. But, regardless of duration, they cannot have three breaks.

- No break can be taken at the very beginning of an employee's shift. This time should be devoted to receiving information from one's colleague(s) on the preceding shift, reading the Communication Notes, etc. And, in the mornings, supported people, who may be waiting for breakfast or for personal care assistance, must take priority.

- In order to avoid missing emergency phone calls, staff are permitted to take their cell phones with them when going out in the community with a supported person(s). However, the device must be kept secreted in the staff's handbag or pocket. Further, texting is not permitted when supporting a person in the community because emergencies are not communicated via text message.

- Employees may also take their personal devices with them when they are attending meetings or training sessions off site. However, regardless of the venue, the devices must be muted during all sessions and employees can only access their messages and/or respond to them during the break times allowed at the seminar, meeting or conference in question.

- If employees choose to bring personal cell phones (or i-phones, blackberries, etc.) into the work place, and if they choose to use them for strictly work related communication, such use is obviously not restricted to break times. It must be noted, however, that in no circumstance will the agency reimburse an employee for damage done to his or her personal IT device.

- Defamatory or libelous comments posted on social media sites about the workplace, its employees, or the people that it supports will be dealt with via the disciplinary process or the courts, as appropriate. CLDN will respond in similar fashion if pictures of supported people are posted on such sites, unless a case specific written consent has been obtained and filed with the agency.

Approved by: Glenn Taylor
CEO

Date: August 9, 2024