



Rationale

This Policy has been developed to ensure that remote work can be accommodated in a safe and secure manner in a home environment. Remote work maybe required or permitted due to health or environmental reasons; such as: there is an issue with the building where no one is allowed to enter for one or more days; the Ministry of Health is encouraging social distancing as part of community efforts to slow the progression of a pandemic.

Policy

Provided that a safe and secure working environment is possible at home, school employees may work from a home environment when the Ministry of Education, the Ministry of Health and/or the CISDV Board of Directors authorizes or encourages employees to work from home.

Definitions:

Working remotely means a situation in which an employee works mainly from home and communicates with others via email, video conferencing and telephone.

Working alone means to work in circumstances where assistance would not be readily available to the worker (a) in case of an emergency, or (b) in case the worker is injured or in ill health. Factors to consider in determining whether an employee is working alone or in isolation:

1. Presence of others: Are other people in the vicinity?
2. Awareness: Will other persons capable of providing assistance be aware of the worker's need?
3. Willingness: Is it reasonable to expect those other persons will provide assistance?
4. Timeliness: Will assistance be provided within a reasonable period of time?

Regulation

1. CISDV Employees

In any circumstances where a CISDV employee will be working remotely:

- a) Employment entitlements and expectations remain the same.



The Employee's work hours; overtime compensation; use of sick leave; approval for use of vacation; requests for a Leave of Absence; and compliance with CISDV policies, procedures, and guidelines remain in effect.

Employees are expected to be available during regularly scheduled business hours, for communication by phone and email and/or on-line platforms. Alternate scheduled business hours may be approved upon written request to the Principal.

If an employee is not available to work on any given day (example: illness, etc.), they are required to inform the Principal.

- b) Employees are expected to maintain a safe and secure work environment.

Employees should designate a remote workspace to accommodate any equipment to be used in their work. If the employee has any ergonomic needs, those should be communicated to the Principal.

Employees should protect their home workspace from any hazards and dangers to their equipment or themselves. This includes having adequate lighting; proper electrical outlets/cable maintenance; functional smoke monitors, fire extinguishers and (if required) carbon monoxide monitors; a first aid kit; and a clean and healthy working environment.

Employees should have an evacuation plan in place from their homes to a safe location in the event of an emergency.

- c) Employees are expected to maintain regular contact with their Principal and/or designate.

On a workday, employees should be in contact with their direct Principal and/or designate a minimum of twice each day, which may include attending virtual meetings, sending emails, checking in through an established method, or making phone calls. This provides for the appropriate check-in procedures.

- The Principal must review the procedures for checking the well-being of workers.



- A person must be designated to establish contact with the workers at predetermined times and the results must be recorded.
- The procedure for checking a worker's well-being must include contact at the beginning and end of the employee's scheduled work day.
- In a case where the worker cannot be contacted, Principal and/or designate will:
 - phone the employee
 - phone the employee's emergency contact
 - failing that, send someone to the employee's home, and
 - failing that, contact police or emergency services.
- Alternate procedures for checking a worker's well-being must be approved in consultation with the worker and school Work Safe Committee.

All employees must ensure that they have supplied their cell phone numbers and emergency contact information to their Principal and/or designate.

Employees should report any emergencies or work-related injuries to their Principal and/or designate within 24 hours or at the earliest reasonable opportunity. Work related injuries are to be reported to WorkSafeBC (WSBC) as per WCBC regulations.

In the event of a medical or other emergency requiring immediate action from fire, police or medical department, employees must dial 9-1-1.

If employees will be working alone in their remote work environment (i.e. if there are no other adults in the residence), then they must inform their Principal and/or designate of that fact.

- d) Employees are expected to maintain professional dress when attending virtual meetings related to work.
- e) Employees must ensure that there are security measures in place to protect CISDV data and information. Employees should be aware of their obligations under the CISDV Technology Policies.



Employees are not permitted to download or store any CISDV data or information onto their personal computers or onto any device other than those provided by the CISDV. Employees also must not forward any such documents to their personal email address.

Employees should take care to ensure that they are the only individuals who are able to access CISDV records and that their devices have appropriate security settings. Some steps include:

- Logging off or shutting down their laptop or home computer when not in use;
- Setting the automatic logoff or lock screen after a short period of idleness;
- Password protection on all devices used to access work related data, including emails (phones, laptops, tablets, computers);
- Ensuring that software, including security software, is up to date;
- Only downloading applications/software from an approved source (i.e. from the device's app store, not from the internet);
- Not sharing a laptop or home computer containing personal information related to work with other individuals, including family members and friends;
- If physical records are at home, storing those records in a location that protects the privacy of students, parents/guardians and staff;
- Avoiding sending personal information by email from public locations or using public WIFI;
- Encrypting any electronic device that stores personal information. This includes but is not limited to home computers, USB flash sticks, laptops and mobile phones; and
- Reporting any suspicious activity (e.g. suspicious emails) *before* clicking on any links.

If any device containing personal information is stolen or lost, employees must immediately notify their Principal and/or designate.

- f) Employees should limit the stress on the CISDV VPN (school Virtual Private Network) system.



Employees should only use the remote system for employment related purposes and should log onto the system only when necessary. Employees should sign off, rather than disconnect, when away from the computer.

In addition, employees should not use the remote system to access streaming videos, unless requested to do so as part of their employment.

2. CISDV Schools:

Schools may consider additional local practices and procedures to ensure the occupational health and safety of employees when working remotely.

<ul style="list-style-type: none"> • Reference: BC Office of Information and Privacy: <ul style="list-style-type: none"> ○ Mobile Devices: Tips for Security & Privacy : https://www.oipc.bc.ca/guidance-documents/1994 ○ Protecting personal information away from the office: https://www.oipc.bc.ca/guidance-documents/1447 • WorkSafeBC: <ul style="list-style-type: none"> ○ Health and safety responsibilities when working from home: https://www.worksafebc.com/en/about-us/news-events/announcements/2020/March/health-safety-responsibilities-when-working-from-home • Government of BC <ul style="list-style-type: none"> ○ Emergency Preparedness for Working at Home: https://www2.gov.bc.ca/gov/content/careers-myhr/all-employees/work-arrangements/flexible-workplaces/emergency-preparedness ○ Safety Inspection for Working at home: https://www2.gov.bc.ca/gov/content/careers-myhr/all-employees/work-arrangements/flexible-workplaces/safety-inspection ○ Flexible Workplaces & Information Security: https://www2.gov.bc.ca/gov/content/careers-myhr/all-employees/work-arrangements/flexible-workplaces/information-security • Canadian Centre for Occupational Health and Safety: <ul style="list-style-type: none"> ○ https://www.ccohs.ca/oshanswers/hsprograms/telework.html 	<p>Approved by CISDV Board of Directors</p> <hr/> <p>Date Approved: June 2, 2020</p>
<p>Cross-reference: Policies: 318 PIPA for Employees and Volunteers 319 PIPA for Parents and Guardians 613 Internet Acceptable Use 614 Personal Computing at Schools 615 Electronic Communications 616 Staff Purchased Computers 617 Social Media</p>	<p>Date(s) Revised:</p>