COMMUNITY FOUNDATIONS OF CANADA | The Learning Institute

Fact Sheet: Working from home

Dec. 16, 2020

The new COVID-19 reality means that many employees are “working from home” (WFH). As a local employer, there are new challenges to navigate, and new normals to integrate into your professional planning.

The following article is reprinted and translated with permission from DLA Piper (Canada) LLP.

Work from home: considerations for employers during COVID-19

WFH is no longer treated as a flexible work option by some employers, but a measure to physically distance. Many employers are now questioning business costs associated with traditional offices altogether, exploring the idea of WFH as a new way to work.

While there are savings and conveniences that come with WFH and virtual offices, there are also employment considerations to keep in mind when making this transition, during the pandemic and beyond. When transitioning to a remote work model, employers should consider how their current workplace policies apply to WFH, including supervision, performance management, time recording, privacy, confidentiality, IT and document management, and insurance. Employers should also be aware of their obligations under applicable legislation, including employment standards, health and safety, and human rights.

Occupational Health and Safety (“OHS”)

Employers continue to have health and safety duties when employees WFH, and employers generally cannot pass-on business costs to employees. Generally, OHS regulations require employers to ensure employees assess their home workspace, report hazards, and follow OHS protocols. A safe workspace includes:

- Emergency procedures, including evacuation and communication protocols in case of emergency;
- Ergonomic assessment and considerations; and
- Check-in procedures for employees working alone.

Further, employers should be cognizant of their responsibilities relating to training and supervising employees when they WFH, and reporting workplace injuries that occur in the home workspace. (note: further in this document there is more detail on OHS and employer’s responsibilities).

Business Costs

Except when permitted by law, employment standards legislation in many provinces generally prohibit employers from passing the costs of doing business onto employees. For this reason, many employers reimburse employees for expenses such as cell phone, travel, computer hardware or software, or automobile maintenance when these costs are incurred for the business.

When employees are required to WFH, employers should also consider if employees are improperly shouldering business costs. This may include, for example, specific computer hardware or software if it is required to perform their work.

One expense that is not often reimbursed by employers, unless agreed by the employee and employer, is the cost of a home office space. This includes, for example, a portion of rent and utilities. However, where an employer does not reimburse the employee, home office expenses may be a tax deduction for the employee.

Employers should ensure that a clear policy or agreement is in place on what responsibilities the employer and employee have with respect to expenses and equipment. A formal arrangement may also support an employee's ability to deduct home office expenses for tax purposes. In that case, an employee may request that the employer complete the CRA Form T2200 *Declaration of Conditions of Employment* to support the deduction. Further details on employee home office expense deductions can be found here.

Large-scale WFH is relatively new territory for many businesses. Any employer implementing WFH, either on a temporary or permanent basis, should conduct a review of its workplace policies, employment agreements, and the applicable laws in their jurisdiction.

This article is reprinted with permission of Koskie Minsky LLP (Toronto) and was written by Barbara Walancik.

Maintaining privacy standards while working from home during COVID-19

With various Canadian provinces and territories declaring states of emergency as a result of the outbreak of COVID-19, many workplaces have directed their employees to work from home. While we live in an era where most businesses are prepared and equipped for their employees to work remotely, there remain a number of challenges in ensuring privacy standards are adhered to and various ways employers and employees can lower risks.

> ***Computer security, cybersecurity or information technology security are all terms used to describe the protection of computer systems and networks from the theft or damage of hardware, software, data, and misdirection of services. Information technology security is a primary concern when working from home.***

Some cybersecurity threats include:

- unsecured home wifi networks
- sensitive data is being shared across wider networks, some of which are not secure
- using personal devices or networks that may not be compliant with corporate standards, may not be up to date or are accessed by others in the home
- heavy reliance on group communication tools, some of which may not be secure
- scams targeting remote workers.

Some ways of addressing the inherent risks associated with working remotely include:

1. **Establish a work from home policy and regular training**

In order to address some of the above risks that come with working remotely a company should establish procedures to be followed when working remotely and ensure proper training of employees to ensure the policy is understood.

This policy and training can address many of the issues that arise when an employee is working remotely including:

- Different security settings depending if the individual is on a wifi network at home or in a more public place like a hotel or coffee shop,
- Ensuring the home router is secure,
- Regular data back-up requirements,
- Training employees on phishing emails and other scams targeting remote workers.

2. Ensure Employees have the right tools

Ensuring employees have the right tools will vary depending on the business, which may include providing a computer to the employee that is strictly to be used for business and that has all the required tools to ensure cybersecurity, or at a minimum ensuring that any computer used remotely has:

- Strong passwords that are regularly changed
- Passwords that are not used across multiple platforms
- Two-factor authentications
- A Virtual Private Network (VPN) which will ensure encrypt network traffic
- Firewalls
- Antivirus software
- Regular updates of all software
- Regular data back up
- Encrypted communication capabilities
- Device locking after a short period of not being used.

Ensuring that employees know how to use the tools they are provided to ensure cybersecurity is important and should not be disregarded.

3. Keeping Records and Personal Information Safe

When dealing with personal information:

- Ensure that security levels are not changed as a result of the transition to working from home when accessing personal information or records
- Limit the records or personal information being taken home by employees to that what is necessary
- Ensure that records or personal information are transported safely – for example, a locked bag for paper records and an office-issued laptop that is encrypted for electronic records
- Paper records, laptops or other devices should not be left in a public place such as a car while an employee runs and errand on their way home (i.e. grocery shopping) and should be stored in a secured location (i.e. a locked filing cabinet, desk drawer or office) at home
- Electronic transmissions of personal information should be secured through encryption with the password provided separately (i.e. over the phone or through a separate email with a clue)
- Paper records, laptops or other devices with records or personal information that are no longer required should be securely returned to the office as soon as they are no longer needed.

4. Guidance Documents

The Office of the Privacy Commissioner of Canada has released a guidance document on privacy issues during a pandemic and addresses both PIPEDA and the Privacy Act, which can be viewed **here**.

Several provincial privacy authorities have also released guidance documents for employees working from home, which can be accessed at the following links:

- **Alberta** – Office of the Information and Privacy Commissioner of Alberta
- **British Columbia** – Office of the Information and Privacy Commissioner for British Columbia
    - See also: Guidance Document: Protecting Personal Information Away from the Office
- **Newfoundland and Labrador** – Office of the Information and Privacy Commissioner
- **Northwest Territories** – Northwest Territories Information and Privacy Commissioner
- **Ontario** – Information and Privacy Commissioner of Ontario
- **Quebec** – Commission d'accès à l'information du Quebec
- **Saskatchewan** – Office of the Saskatchewan Information and Privacy Commissioner
- **Yukon** – Yukon Information and Privacy Commissioner

Additional Information

Work from home safety risks

Small business insurance coverage, including general liability, property and workers' compensation, will protect workers while at the worksite, office or at home. Workers' compensation insurance generally covers if an employee is hurt during business hours while working from home.

However, workers' comp rules will vary by province. Working from home can facilitate unique workers' compensation risks, including:

- Ergonomically unfriendly work areas
- Awkward (aka shared) workspaces
- Cybersecurity risks

Prevent risks by following work from home safety tips:

A key best practice to ensure safety and reduce Workers' Compensation claims is to establish protocols for working from home that will help to mitigate the possible risks. The policy should incorporate risk management guidelines that tie in with work from home policy requirements listed above, including:

- **Create a workspace:** Employees should find a dedicated workspace where they can focus on their work with minimal distractions. To help mitigate problems, have your employees who will be new telecommuters to test their at home technology now before it becomes a necessity. It is usually not just as simple as plugging in a computer.
- **Inspect the work area:** A home workspace should be inspected to make sure it is free from any hazards, including fire and ventilation issues, slipping and falling dangers and other daily risk factors.
- **Teach injury prevention:** Make sure all employees understand how to prevent workplace injuries both in the workplace and at home.

Here is a link to a great safety checklist for working at home: https://telework.gov/federal-community/telework-employees/safety-checklist/. While it is U.S. based, it's generic enough to apply to any country.

Provincial and territorial workers compensation boards:

- **Alberta** — wcb.ab.ca
- **British Columbia** — worksafebc.com
- **Manitoba** — safemanitoba.com
- **New Brunswick** — worksafenb.ca
- **Newfoundland and Labrador** — workplacenl.ca
- **Nova Scotia** — worksafeforlife.ca
- **Northwest Territories** — wscc.net/ca
- **Nunavut** — wscc.net/ca/
- **Ontario** — wsib.ca
- **Prince Edward Island** — wcb.pe.ca
- **Quebec** — csst.qc.ca
- **Yukon** — cfib-fcei.ca