

ELECTRONIC COMMUNICATIONS POLICY

OBJECTIVE

The availability and use of electronic communication and collaboration tools, both internal and external, is on the rise. These tools provide new and emerging opportunities for employees to communicate with coworkers, customers, and the public to inform, share, collaborate, and learn. This policy covers all electronic communication and collaboration tools and the content generated by these tools. These tools include voice mail, e-mail, video conferencing, social media tools, the internet, the intranet (WSN) when accessed through any WorkSafeBC or employee-owned equipment or devices such as telephone, mobile phones (smart phones), or computer.

The main purpose in adopting and deploying these tools at WorkSafeBC is to enhance WorkSafeBC business communications. This policy provides a framework for the professional use of all electronic communication and collaboration tools to advance WorkSafeBC's vision, mission, and mandate.

New electronic communication and collaboration tools can give communications a much greater impact than ever before. While generally positive, using electronic communication and collaboration tools involves certain inherent risks.

The policy is also intended to help employees manage the risks to themselves, coworkers, the organization and its customers that can come with the use of these tools, and is meant to be applied in conjunction with the Standards of Conduct and the Corporate Ethics Program, the Harassment Policy, the Privacy Policy and other applicable policies, guidelines, and procedures.

By their very nature, electronic communication and collaboration tools will continue to evolve. Employees are expected to generalize from the principles, guidelines, and examples presented here and apply them even in situations not expressly discussed. This policy may be amended from time to time to fully reflect the changing environment.

APPLICATION AND SCOPE

This policy applies to all permanent and temporary employees at WorkSafeBC who use any electronic collaboration or communication tool through any WorkSafeBC equipment or devices at any time.

The policy also applies when electronic communications are published or sent to external parties from WorkSafeBC equipment or devices and personal equipment or devices where at least one of the following criteria is met:

- It refers to WorkSafeBC work
- It identifies the sender of the communication as a WorkSafeBC employee
- It refers to a WorkSafeBC employee or his/her work
- It directs people to a WorkSafeBC internet site

WorkSafeBC Electronic Communications Policy *(continued)*

For the purpose of this policy, the term “employee” includes those contractors and consultants who provide services to WorkSafeBC through a contract for services and their respective employees.

DEFINITIONS

Content — includes communications, information, and data held in electronic collaboration and communication tools.

Electronic communication tools — includes the internet and systems and applications that allow access to the internet, as well as systems and applications that allow for interactive online communication. Examples include, but are not limited to, electronic meeting tools like Live Meeting, instant messaging (Office Communicator), texting, e-mail, personal information management tools like Outlook, mobile devices (mobile/smart phones), and social networking applications like Twitter, Facebook, and LinkedIn.

Electronic communications — includes all forms of online communication and any attached information and data. This form of communications will continue to evolve and current examples include e-mails, instant messages, online chat, texts, voice mails, podcasts, online videos, and posts to blogs, vlogs, and wikis.

Personal information — is any information about an identifiable individual, other than business contact information, that is recorded in any format. It can include an individual’s home address, home phone number, race, religion, ethnicity, sexual orientation, age, birth date, weight, height, medical history, employment history, educational history, and/or character references.

WorkSafeBC information — has the same meaning as that attributed to the term in the *Undertaking of Confidentiality* and includes all information held by WorkSafeBC that is not generally available to the public.

POLICY SUMMARY

Electronic communication tools have been implemented to make business communication, both within WorkSafeBC and with outside individuals and organizations who do business with WorkSafeBC, more efficient and effective.

WorkSafeBC employees are expected to use these tools to inform, share, collaborate, and learn within the context of their jobs and professional activities.

Employees are required to use these tools in a lawful and ethical manner and are expected to exercise good judgment consistent with the values and principles set out in the *WorkSafeBC Standards of Conduct*. Employees must communicate responsibly, demonstrate respect, and manage their impact in order to protect the reputation of WorkSafeBC, themselves, their coworkers, WorkSafeBC customers, and others.

In their electronic communications, employees are obligated to respect the rights and reasonable interests of others, including privacy and confidentiality rights, human rights, and proprietary, copyright, and other commercial rights.

WorkSafeBC owns all electronic communications and content held in electronic communication tools owned by WorkSafeBC. This ownership includes all communications and content relating to business or personal matters and those items marked as private, personal or confidential.

WorkSafeBC may apply restrictions on the access to, and use of, electronic communication tools by employees within local areas and/or across the organization to ensure efficient operations and superior customer service.

Where required for business purposes (e.g. investigations, audits), management may authorize employees to depart from the terms of this policy.

Contravention of this policy may lead to discipline up to and including termination of employment or termination of a contract for services.

DETAILED POLICY POINTS

A. Demonstrating responsible use

1. Follow the WorkSafeBC Standards of Conduct

This policy is rooted in the *WorkSafeBC Standards of Conduct*. The same principles and standards that apply to WorkSafeBC employees in their day-to-day work also apply to activities conducted in or through electronic systems. If you are uncertain whether a particular communication meets one of the Standards, delay your communication and seek guidance from your manager or the Office of the Chief Ethics Officer through the Ethics Office (SM).

When using tools connected to or through the internet, you must also follow the principles and restrictions set out in the *Internet Usage Agreement*, which employees sign upon starting work at WorkSafeBC.

2. Protect WorkSafeBC information and respect privacy rights

Due to the nature of our work, a great deal of information at WorkSafeBC is protected by statute from disclosure to the public, except in specific circumstances. Electronic communication tools may encourage a sense of familiarity that lulls users into sharing information generously, and this can be dangerous for our customers, our coworkers, and the organization. Be cautious about what information you share in your communications, especially regarding personal and sensitive information about customers, as well as personal information about yourself.

You must follow the restrictions and principles laid out in the *Undertaking of Confidentiality*, which employees sign upon starting work at WorkSafeBC. Employees are responsible for the proper use, management, and storing of WorkSafeBC data and information regardless of whether the electronic communication or data is created, saved or copied onto or communicated through WorkSafeBC or personal equipment and devices.

If e-mail is used to send WorkSafeBC information or personal information externally, then appropriate security measures such as encryption must be used. WorkSafeBC information and/or personal information must not be transmitted via or exposed to electronic systems connected to the internet without security products and protocols approved by the Information Security Architecture and Operations Department in place.

If in doubt about whether information is WorkSafeBC information or personal information, confirm its status with your manager before you communicate about it.

3. Comply with requirements of the FIPP Act

Electronic communications are records under the *Freedom of Information and Protection of Privacy Act* (FIPP Act), and consequently all the FIPP Act requirements and rules around collection, use, and disclosure of personal information may apply. Deleting an electronic communication is similar to shredding a paper document. Electronic communications which constitute a business transaction or decision, such as adjudication decisions, payment approvals, travel authorization, etc., must be saved in an appropriate file, whether paper or electronic.

Electronic communications containing personal information used to make a decision affecting an individual must be kept for a minimum of one year. If all pertinent information from a transitory electronic communication has been transferred to a permanent record there is no requirement to keep the original record for any period of time (and deletion is encouraged). If a relevant electronic communication exists at the time a FIPP request is made, that electronic communication cannot be destroyed for any reason, even if the information has been transferred to another permanent medium.

The FIPP Act prohibits storage of or access to personal information outside of Canada except in limited circumstances. When travelling outside of Canada, do not access personal information in WorkSafeBC systems unless necessary for business purposes. Never transmit personal information outside of Canada without the express consent of the individual the information is about, or the review and approval of the FIPP Office.

4. Report privacy breaches

Where you see that personal information has been disclosed through an electronic communication inadvertently or without authorization, you are required to report this as a privacy breach to your manager as soon as possible. Managers must in turn, immediately notify the WorkSafeBC [FIPP office](#) by telephone (604 279-8171) or in writing through the Privacy Breach Notification Form.

5. Protect passwords, accounts, and electronic communications

Take reasonable steps to maintain the security and the integrity of your mailboxes, accounts, profiles, and their contents. Do not leave your personal computer, laptop, or other WorkSafeBC devices, unattended, logged-on, or in an unlocked state or communicate your security password(s) to others. Do not grant access to others to your mailboxes, accounts, or profiles except for legitimate business reasons as approved by your manager. Appropriately secure any electronic communications that you archive or export from any communication tool.

6. Respect the intellectual property of others

Recognize and honour the intellectual property of others, and use due diligence to comply with all applicable laws and regulations and the legal protection provided by copyright, patents, trade-marks, licenses, and other proprietary rights. You are specifically prohibited from using WorkSafeBC equipment or devices to obtain or share copyrighted content such as music, movies, games or software without the permission of those who hold the proprietary rights to the content. Even where such permission has been received, you must not download or install software of any kind to WorkSafeBC equipment or devices unless you have been authorized to do so. WorkSafeBC does

permit the downloading and installation of software on some portable devices such as smart phones but some restrictions apply.

7. *Proactively respond to health and safety risks*

While this policy provides guidance for your role as an employee, it is also important for you to consider your personal safety outside of work. In order to proactively mitigate risks at home which may flow from employment, such as threats of violence, give careful consideration to what personal information you post online, in particular on social media sites, including where you live and work. This information may be used against you by people with unlawful or improper intentions.

If you see a contravention of this policy that involves a health and safety risk to any individual, report it immediately to your manager. Report any other contravention of this policy to your manager or to HR Initiatives (SM).

B. Managing your personal use during business hours

During working hours, employees must avoid using electronic communication tools for personal use. This restriction applies to systems and devices owned by WorkSafeBC and also those owned by employees, and use includes, amongst other activities, internet surfing, texting, and video streaming.

Electronic and online activities related to personal business or interests are only permitted during your break periods and time before and after work. In the rare case where a personal matter is pressing and unavoidable, occasional and brief personal use of these tools is acceptable provided the terms of this policy are strictly followed.

Employees should be careful to understand that during working hours, you are paid to focus exclusively on work. Where necessary, WorkSafeBC will monitor usage of all electronic communication tools, and specifically the internet, and may take disciplinary action against employees whose usage patterns indicate that they have contravened this requirement. If you are uncertain about what constitutes acceptable use of electronic communication tools in your department during working hours, you should proactively seek clarification from your manager.

C. Demonstrating respect and managing your impact

1. *Avoid offensive materials, sites, and communications*

You must avoid accessing or attempting to access sites, participating in online activities or sending electronic communications that might in any way discredit WorkSafeBC. This includes sites and electronic communications which contain offensive material, or which disseminate information that is illegal, defamatory, abusive, racially offensive, and/or sexually explicit. You must not display, archive, store, distribute, edit or record offensive material on any WorkSafeBC device or equipment.

2. *Choose your language carefully to demonstrate respect*

Be thoughtful and respectful in your communications. You should recognize and respect the diversity of the population, and respect the opinions of others. Know that conversations may be recorded or filmed and that these recordings may be placed on social media sites with or without your knowledge. This possibility should assist in guiding your actions. Avoid exaggeration, colourful language, guesswork, obscenity, inflammatory or objectionable content, copyrighted materials, legal conclusions,

derogatory remarks or personal characterizations. Some communications may be so offensive or obscene that even as personal expression they undermine WorkSafeBC's reputation and interests and may contravene this policy.

3. *Don't hide behind anonymous communications*

Online communications can remain posted for an indefinite period, and you may lose the ability to edit, change or delete your communication, so consider your content carefully. Some users think they can communicate anonymously in order to express their views. However, almost no postings are truly anonymous on the internet; you should not use anonymity as a shield for disrespectful or harmful content.

4. *Speak for yourself*

When communicating, identify yourself, speak in the first person and be sure that the communication reflects your own point of view. Don't claim or imply that you speak for WorkSafeBC unless authorized by your manager to do so.

5. *Use a disclaimer*

In any external communication where you have not received authorization to speak on WorkSafeBC's behalf, and where you refer to WorkSafeBC work, identify yourself as a WorkSafeBC employee, refer to a WorkSafeBC employee or his/her work, or direct people to a WorkSafeBC site, you are required to communicate the following disclaimer, or something materially similar, in a reasonably prominent manner: "The views expressed here are mine and do not necessarily reflect the views of WorkSafeBC." Your communication should not include WorkSafeBC logo or trademarks.

6. *Manage the impact of your position and status*

Sometimes employees are so closely associated with the organization due to their role, power, and influence that even using a disclaimer will not render their comments exclusively personal in nature. Because a greater degree of scrutiny and accountability attaches to their roles, these employees should use extreme care in selecting the content of their communications.

7. *Direct concerns and complaints internally first*

Beware of venting about work matters online. You are encouraged to express your concerns or disagreement with WorkSafeBC actions or policies by sharing your thoughts through formal channels internally and giving the organization a reasonable opportunity to consider your views and respond. If you are uncertain about where to direct your concern, seek guidance from your manager or HR advisor on which channel will get to the essence of your concern most quickly.

8. *Don't communicate with the news media unless authorized*

Follow the same general guidelines and judgment when making external electronic communications that now guide your actions with other media, including television, radio, magazines, newspapers, and any other release of information to the public. Your external communications may generate public and news media interest. Unless you are expressly authorized to speak for WorkSafeBC, all requests for comment from the news media should be forwarded to the director of communications or the director of media relations in the Communications Department at 604 276-3141.

D. Tool usage and monitoring

WorkSafeBC may monitor employee use of the electronic communication tools to ensure employees are in compliance with the terms of this policy. WorkSafeBC retains the right to access and view all electronic communications and content, including all items relating to business or personal matters and those items marked as private, personal or confidential.

Use of WorkSafeBC electronic communication tools constitutes consent to the monitoring and recording of all electronic activity, including but not limited to internet sites and communication tools accessed, content viewed, created, sent and/or posted, and time spent using the tools.

WorkSafeBC may apply restrictions on the access to, and use of, electronic communication tools by individuals or groups of employees within local areas and/or across the organization where necessary to ensure appropriate and productive use of work time by all employees, efficient operations, and superior customer service.

WorkSafeBC will only access a mailbox assigned to an employee in limited circumstances. Examples include:

- Suspicion of fraud
- Misuse of corporate resources — e.g. use of WorkSafeBC's e-mail system to run a personal business
- The rare circumstance of a pressing business need during the unexpected absence of an employee
- Investigation of a disciplinary matter

OTHER APPLICABLE POLICIES OR REFERENCES

Harassment Policy

Internet Usage Agreement

Privacy Breach Response Protocol

Undertaking of Confidentiality

WorkSafeBC Standards of Conduct and Corporate Ethics Program

EFFECTIVE DATE

This policy takes effect on September 30, 2010.

ADMINISTERED BY

This policy is administered by the Corporate Human Resources Initiatives and Services Department.