



Standards of Conduct for Community Living British Columbia Employees

These *Standards* establish the expectations for conduct and behavior of all CLBC employees. They form a condition of employment and must be reviewed and signed by each employee upon hire, and whenever they are significantly revised.

The *Standards* are designed to both protect employees and further the mission, vision and values of the organization. Failure to sign or comply with these *Standards* is grounds for disciplinary action, up to and including dismissal. Questions about the application or interpretation of these *Standards* should be directed to People Services.

Values

CLBC is a values- and performance-based organization. Our mission and vision drive what we do every day. Our values form the building blocks of our behavior – the guide for our interactions with individuals, families, service providers, each other and the public. Employees use these values as a daily touchstone and as a lens for their actions and decisions.

Ethical Conduct

As a crown corporation, CLBC is charged with delivering public services for vulnerable adults and their families. This requires the highest standards of ethics, integrity and accountability, in order to protect the interests of those we serve, and the public of B.C. Employees must conduct themselves professionally, be fit for duty, and be free from impairment (e.g. from alcohol or drugs).

Loyalty

Employees have a duty of loyalty to their employer. They carry out their duties in an honest and impartial way that is above suspicion; maintains and enhances the public's trust and confidence in CLBC; and does not bring CLBC into disrepute.

Our **vision** answers the question: What are we trying to achieve?

*Lives filled with possibilities
in welcoming communities.*

Our **mission** answers the question: How are we going to achieve our vision?

- *Community Living BC serves adults with developmental disabilities as well as those with a diagnosis of Fetal Alcohol Spectrum Disorder or Autism Spectrum Disorder who meet the eligibility criteria.*
- *In collaboration with our stakeholders, we facilitate and manage a responsive, sustainable network of disability-related services that supplement other supports to assist adults with developmental disabilities to live good lives and be full participants in their communities.*
- *We offer a range of options in the way services and supports are provided to the individuals we serve. The options provide for choices that allow services and supports to be tailored to the circumstances and preferences of each individual.*
- *We take a holistic approach that acknowledges the supports and responsibilities of all stakeholders including individuals, families, service providers and community resources. This collaboration supports individuals to achieve the best possible outcomes.*

Our **values** answer the question: What will guide our actions?

- *Our interactions are respectful and transparent*
- *We use an equitable approach that is person-centred and effective*
- *We use consistent processes and tools*
- *We adopt proven new methods that align with our goals*

Confidentiality and Privacy of Personal Information

In the course of their work, employees collect and use sensitive and personal information about the organization, the people we serve and other employees. Employees protect and respect the confidentiality of such information consistent with requirements under BC's *Freedom of Information and Protection of Privacy Act* (FOIPPA).

Confidential information, in any form, that employees receive through their employment must not be divulged to anyone other than persons who are authorized to receive the information. Employees who are in doubt as to whether certain information is confidential must ask the appropriate authority before disclosing it. Caution and discretion in handling confidential information extends to disclosure made inside and outside of government and continues to apply after the employment relationship ceases.

Confidential information that employees receive through their employment must not be used by an employee for the purpose of furthering any private interest, or as a means of making personal gains. See the Conflicts of Interest section of this document for details.

Intellectual Property

All Intellectual Property including systems, courseware, methods, programs and related development created during the course of employment is considered to be the property of CLBC.

Public Comments

CLBC employees are free to comment on public issues as long as they do not jeopardize the perception of impartiality in the performance of their duties. CLBC employees do not use their position in CLBC to lend weight to the public expression of their personal opinions, and exercise care in making comments or entering into public debate regarding CLBC policies.

Political Activity

CLBC employees are free to participate in political activities, including belonging to a political party, supporting a candidate for elected office and seeking elected office. Employees clearly separate their political activities from activities related to their employment by:

- Impartiality in relation to their duties and responsibilities
- Avoiding engaging in political activities during working hours
- Not using CLBC facilities, equipment or resources in support of these activities
- Not introducing partisan politics at the local, provincial or national levels into the workplace, except in the form of informal private discussions among co-workers

Service to the Public

CLBC employees are respectful, courteous, professional, fair, efficient and effective in their provision of public services. Employees are cooperative, flexible and responsive to the changing needs, expectations and rights of the people we serve and a diverse public, while respecting the legislative and policy framework within which those services are provided.

Workplace Behaviour

CLBC proactively maintains and expects a respectful and positive workplace that supports the productivity and wellbeing of both employees and the individuals we support. Employees have a right to expect such a work environment, and the responsibility to behave accordingly. They understand and comply with CLBC policies about respectful workplace behavior.

Conflict of Interest

As a key element of a high ethical standard, CLBC takes a transparent and proactive approach towards real, perceived or potential conflicts of interest involving employees. While recognizing that conflicts sometimes exist, and that employees enjoy the same rights as other citizens in their private dealings, CLBC manages any conflicts so as to protect the interests of the individuals we support, and the integrity of the organization. Employees understand and comply with CLBC policies relating to conflict of interest.

Ethical Reporting Policy

CLBC strives to achieve the highest standards of ethical, moral and legal conduct. As such, CLBC encourages the reporting of irregularities, including fraud, theft and corruption that impacts either CLBC or individuals supported. CLBC is committed to protecting the identity of whistleblowers and persons cooperating in the investigation of irregularities, except when legally prohibited. Employees are aware of and comply with CLBC policies relating to Ethical Reporting.

Legal Proceedings

Employees may from time to time encounter legal documents, investigations or proceedings in the course of their work. These may include search warrants, summons, subpoenas, orders or requests for records. In such situations, employees comply with CLBC policies related to legal requirements, ensuring that appropriate legal counsel is consulted before responding. Employees cooperate with legal counsel acting for CLBC during legal proceedings.

Policy References

(This list is not exhaustive and may change from time to time)

- BCGEU Collective Agreement Article 32.17 (regarding disclosure of information)
- CLBC Values
- Conflict of Interest Policy – Employees
- Ethical Reporting Policy
- Legal Requirements Policy
- Managing Conflict of Interest: A Practice Guide for Employee
- Occupational Health and Safety Program Policy
- Operational Privacy Policy and related Privacy Policy Suite
- Post-Employment Restrictions for Executives Policy
- Respectful Workplace Behaviour Policy
- Workplace Impairment Policy

DECLARATION

I, _____, acknowledge and declare that I have read the above *Standards of Conduct for Community Living British Columbia Employees*, and the related policy references, and agree to adhere to them.

I also agree to take responsibility for reviewing and following any future new and revised policies that pertain to my conduct and behavior as a CLBC employee.

Date

Signature

Date

Signature of Witness

Please forward signed copy to People Services for Employee File.



Policy Number:	Policy Section: People Services	Effective: May 2019
Title: Workplace Impairment Policy		Executive Sponsor: Vice-President, Corporate Services

1. PURPOSE

This policy is part of CLBC's commitment to provide a safe workplace. It specifically addresses issues that may impair people's ability to perform their work. Impairment in the workplace can affect workplace health, safety and service and can come from many different sources, including:

- Prescription and over-the-counter medications
- Illegal drugs
- Alcohol
- Cannabis
- Medical conditions
- Fatigue

2. DEFINITIONS

Employee: is someone who is employed directly by CLBC.

Manager/Supervisor: is an employee of CLBC who is responsible for supervising the work of others.

"Fit for Duty": is a physical, mental and emotional state which enables employees to perform their job tasks competently and continuously in a manner which does not compromise the integrity of CLBC or create a safety hazard to themselves or others.

3. POLICY

Promoting workplace health and safety is the responsibility of all employees.

Employee Responsibilities

To ensure everyone's safety, all CLBC employees must:

- Read, understand and comply with the [Standards of Conduct](#)
- Read, understand and comply with the [Occupational Health and Safety Program Policy](#)
- Report to a supervisor if they may be impaired, or not fit for duty, for any reason
- Report to a supervisor if they observe another employee who may not be fit for duty

Employees who have medical conditions, substance addiction issues or require medications which may impair their ability to work safely should provide a Doctor's Certificate to their manager/supervisor that outlines the limitations or restrictions and any accommodation that may be required.

Manager/Supervisor Responsibilities

As a manager/supervisor, you have a responsibility to monitor for impairment in the workplace and address any impairment issues to ensure a safe, healthy, productive workplace. All managers/supervisors must:

- Be knowledgeable about and comply with the [Standards of Conduct](#) and the [Occupational Health and Safety Program Policy](#)
- Ensure employees are aware of and understand Standards of Conduct and Occupational Health and Safety Program Policy
- Understand 'fit for duty' as it applies to your workplace and recognize the signs of impairment
- Have timely conversations with employees if they show signs of impairment and/or substance use dependency and take action and report to People Services when an employee reports impairment or you observe signs of impairment
- Be familiar with the resources and supports available to assist you including the *Manager/Supervisor Guide to Workplace Impairment* and *Manager/Supervisor Q&As on Workplace Impairment*

People Services Responsibilities

- People Services will provide guidance to managers regarding any situations of reported impairment.
- People Services will document any reports of impairment in the workplace and actions taken.

Employees who have a substance addiction are encouraged to contact the [Employee and Family Assistance Program](#).

If you have any questions about workplace impairment, talk with your supervisor.

4. REFERENCES

- Occupational Health and Safety Regulation, BC Reg 296/97 ("OHSR").
- Human Rights Code, RSBC 1996, c 210 ("HRC").
- WorkSafe [Guide to managing workplace impairment and developing an impairment policy](#), 2018
- Public Service Agency [Impairment policy and resources](#) 2018

DECLARATION

I, _____, acknowledge and declare that I have read the above *Workplace Impairment Policy*, and agree to adhere to it.

I also agree to take responsibility for reviewing and following any future new and revised policies that pertain to workplace impairment.

Date

Signature

Date

Signature of Witness

Please forward signed copy to People Services for Employee File.

INFORMATION & COMMUNICATION TECHNOLOGY (ICT) AGREEMENT

Community Living British Columbia (“CLBC”) uses information and communication technologies (“ICT”) to support employees in efficiently delivering services to citizens.

Proper usage of these technologies and associated equipment (e.g. computers, smartphones, iPads, email, information systems, and network) saves time and money, reduces administrative overhead and improves our capacity to respond. Improper usage may jeopardize system integrity and security as well as increasing the risk to CLBC if information is used or released inappropriately.

All ICT resources are provided as business tools to users and are the property of CLBC. Usage is subject to the same restrictions and review process as any other CLBC resource provided to conduct business.

1. Users of ICT resources must:
 - Comply with all applicable legislation, regulations, policies and standards, including the *Standards of Conduct for Community Living British Columbia Employees* and the *Respectful Workplace Behaviour Policy*;
 - Respect copyright and other intellectual property rights in relation to both programs and data;
 - Ensure their usage does not detrimentally affect the productivity, integrity or security of ICT systems and/or harm CLBC’s reputation;
 - Use only the email account provided by CLBC when exchanging email with outside systems.
2. Employees may use Government Internet services for personal use outside of scheduled work hours, provided that such use is consistent with professional conduct and is not for personal financial gain.
3. Reasonable, incidental use of the internet, text and/or instant messaging, email and social media for personal purposes is acceptable during work hours, as long as it does not reduce the employee’s productivity or jeopardize the integrity and security of ICT systems and/or harm CLBC’s reputation.
4. Users of ICT resources must not:
 - Divulge, share or compromise their own or another’s authentication credentials;



- Transmit, post or otherwise expose sensitive CLBC information or personal information to the Internet;
 - Use the ICT resources for commercial solicitation or for conducting or pursuing their own business interests or those of another organization;
5. Send rude, obscene or harassing messages that embarrass, insult or bully individuals;
- Send, forward or reply to large distribution lists concerning matters not related to CLBC business. In addition, users must consider the impact on the network when creating and using large, work-related distribution lists;
 - Attempt to circumvent or subvert system or network security measures;
 - Attempt to obscure the origin of any message or download material under an assumed Internet address;
 - Propagate viruses knowingly or maliciously;
 - Distribute hoaxes, chain letters, or advertisements;
 - Access Internet sites that might bring CLBC into disrepute or harm CLBC's reputation, such as those that carry offensive material.
6. Managers must ensure that all staff sign an ICT Agreement before access to CLBC or government ICT resources is allowed.
7. The Office of the Chief Information Officer (OCIO) monitors the use of government networks and may scrutinize selected network traffic or Internet sites at the request of CLBC. Monitoring is done for operational reasons (e.g., to resolve problems, to identify potential liabilities, etc.).
8. Any content created or transmitted using CLBC/Government equipment or retained within the network will be managed as a government record. There is no expectation of personal privacy related to the use of government information technology resources except for specific privileged communications (i.e. Cabinet, solicitor/client, employee medical documentation and union representative communications).
9. Allegations of inappropriate use of ICT resources will be reviewed by CLBC on a case-by-case basis and may result in a disciplinary process or legal action.

I, _____, have read and agree to follow the terms and conditions as outlined in this *Information and Communication Technology (ICT) Agreement* and the *Appropriate Use of Government Information and Information Technology Resources Policy* (located on CLBC's Intranet).

Employee Signature

Date

Policy Number: IT5.070	Policy Section: Information Technology	Effective: January 5, 2021
Title: Appropriate Use of Government Information and Information Technology Resources Policy ("Appropriate Use Policy")		Executive Sponsor: VP, Information, Technology & Workplace Solutions

1. PURPOSE

This policy describes Community Living British Columbia's (CLBC) approach to Government Information and Information Technology (IT) resources. It is intended to meet the requirements for accessing and managing Government Information (particularly Confidential Information); and using IT resources. It is also intended to meet the security requirements of the *Freedom of Information and Protection of Privacy Act* (FOIPPA), the *Information Management Act*, the *Electronic Documents Act*, and the *Interpretation Act*.

This policy is in accordance with B.C. Government requirements outlined in the *Core Policy and Procedures Manual* (CCPM), *Chapter 12 - Information Management* and *IT Management* and *Chapter 15 - Security*.

This policy supports the protection of privacy and security of individuals and families, service providers, and corporate information. It enforces the protection of the B.C. Government and CLBC infrastructure (cybersecurity) and supports the *Information and Communication Technology Agreement* that all CLBC employees and contractors agree to as part of their CLBC onboarding process. Compliance with this policy and related policies and procedures, as outlined in the Reference section of this policy, ensures that Government Information is appropriately protected while remaining accessible to those who need it and are authorized to access it.

2. DEFINITIONS

Confidential Information: A category of Government Information (including all CLBC information) with confidentiality requirements. It includes, but is not limited to:

- Ministry/Agency confidences (for example, a briefing note to the Minister);
- Government economic or financial information (for example, information about a proposed administrative plan that has not yet been implemented or made public);
- Information harmful to intergovernmental relations (for example, information received in confidence from another government);

- Third Party business information, where its disclosure could harm the third party;
- Personal Information; and
- Legal advice or law enforcement information.

Device: An IT resource that can connect (wired, wireless or cellular) to the government network, including but not limited to computers, iPads, smartphones, and multifunctional devices.

Employee: An individual who is employed directly by Community Living British Columbia (CLBC).

Government Information: All recorded information relating to government business, regardless of format, that is received, created, deposited or held by any ministry, agency, board or commission reporting or responsible to the Government of British Columbia.

Information Incident: A single or a series of unwanted or unexpected events that threaten privacy or information security. Information incidents include the unauthorised collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate.

IT Resources: Information and communication technologies that include, but are not limited to, information systems, Devices, and the government network.

Least Privilege: A principle requiring that each subject in a system be granted the most restrictive set of privileges (lowest clearance) needed to perform their employment duties. The application of this principle limits the damage that can result from accident, error or unauthorized use.

Need-to-Know The legitimate requirement to know, access or possess personal information that is critical to the performance of an authorized, assigned task, and restricted to authorized employees and/or contractors that require it to carry out their work. Employees are not entitled to access merely because of status, rank, or office.

Personal Information: Information recorded about an identifiable individual, including, but not limited to:

- Name, address, telephone number, email;
- Race, national/ethnic origin, colour, religious or political beliefs or associations;
- Age, sex, sexual orientation, marital status;
- Identifying number or symbol such as social insurance number or driver's licence number;
- Fingerprints, blood type, DNA prints; and
- Health care history;
- Educational, financial, criminal, employment history; and

- Anyone else's views or opinions about an individual and the individual's personal views or opinions unless they are about someone else.

Personal information also includes separate pieces of information that may seem unrelated, but when put together would allow someone to accurately infer information about an individual.

Protected Government System: A computer system in a data centre that has met the approved security requirements for the storage of Confidential Information (for example, an Employee's network drives). This does not include the hard drives of computers, iPads, smartphones, or other Devices.

Records: All materials regardless of type or format including but not limited to books, documents, reports, photographs, letters, papers, assessments, plans, notes, electronic methods of communication such as email or fax, audio or video tapes, film and information stored in CLBC information systems whether in writing, electronically, mechanically or by other means.

Third Party: A person or organization other than the person or organization requesting the information.

3. POLICY

Through the appropriate use of government and CLBC information and IT resources, CLBC delivers effective and efficient services to individuals and families while meeting its statutory obligations to protect information.

Where CLBC does not have a policy regarding a specific Government Information or IT resource area, core government policy will apply.

CLBC employees sign the *Standards of Conduct for Community Living BC Employees* upon hiring, and must comply with these standards at all times, including when:

- a. Collecting, accessing, using, disclosing or disposing of Government Information and refer to CLBC's *Organizational Privacy Policy* when Personal Information is involved;
- b. Using IT resources, whether that use is directly related to their employment duties or not; and,
- c. Accessing Third Party hosted sites (e.g. Facebook and Twitter) in a manner that could be perceived as representing government.

Collection, Access, Use, Disclosure, Storage and Disposal of Government Information

Employees must collect, access, use, disclose and dispose of Government Information in accordance with B.C. government and CLBC policies and laws, including the *Information Management Act*, *FOIPPA*, and the *Electronic Transactions Act*.

Employees must store electronic records that relate to government and CLBC business in Protected Government and/or CLBC systems.

Employees **must not** collect, access, use, disclose or dispose of Confidential Information unless authorized to do so and is necessary for the performance of their duties. Employees must adhere to CLBC's *Information Incidents including Privacy Breaches Policy* and supporting documentation when an Information Incident occurs.

Use and Disposal of Government and CLBC IT Resources

Reasonable personal use of government and CLBC IT resources by employees is permitted.

Personal use is reasonable provided that it:

- a. Is limited during core business hours and does not interfere with the employee's duties and responsibilities;
- b. Is lawful;
- c. Does not compromise the security of government and CLBC IT resources or Government Information; and
- d. Is not used for personal financial gain.

Employees must limit the amount of personal records they store on government systems for privacy reasons and to reduce the cost of electronic storage for government.

Employees must use their government email accounts when conducting government business, including while working outside of the workplace.

Employees must not disclose, share, or compromise their own or another employee's government authentication credentials (e.g., passwords, access cards, etc.). This includes not sharing passwords for technical support.

Employees must report any lost or stolen device or access card in accordance with the [General Incident or Loss Report](#) process, and follow CLBC's *Information Incident including Privacy Breaches Policy*.

Employees must comply with CLBC's *Information Technology Asset Management Policy* when disposing of IT resources by following the B.C. Government's [IT Asset Disposal process](#).

Access to and Use of Applications and Software

Employees **must not** download or use applications or software for government business that are not approved or supported by the Office of the Chief Information Officer and CLBC's Information Security Officer.

Employees are not permitted to download or use applications or software that:

- a. Are prohibited by the B.C. Government's Chief Information Officer;
- b. Present unacceptable privacy or security concerns; or
- c. Impose unacceptable terms and conditions.

Monitoring and Investigations

Any collection, access, use, transmission, or disposal of Government Information or use of IT resources, whether for personal reasons or not, may be audited, inspected, monitored, and/or investigated to:

- a. Maintain, repair, and manage IT resources for the efficient operation of business systems;
- b. Meet legal requirements to produce information;
- c. Ensure accessibility of government IT resources for the continuity of work processes;
- d. Improve business processes and manage productivity; and
- e. Ensure compliance with legislative and policy requirements, including the [*Standards of Conduct for Community Living BC Employees*](#).

Allegations of inappropriate access, collection, use, disclosure, or disposal of Government Information or inappropriate use of government IT resources will be investigated on a case-by-case basis. Investigations may include, but are not limited to, the search and/or seizure of IT resources.

Employees who inappropriately access, collect, use, disclose or dispose of Government Information or inappropriately use government IT resources may be subject to disciplinary action, including dismissal, cancellation of contract, and/or other legal remedies.

4. PROCEDURES

All CLBC employees have varying responsibilities when appropriately using Government Information and IT resources to deliver effective and efficient services.

4.1 Vice President, Corporate Services Responsibilities

The Vice President, Corporate Services is responsible for ensuring that CLBC specific policy and procedures are developed, where necessary, to support the *Appropriate Use Policy*.

4.2 Director, Information Technology Responsibilities

The Director, Information Technology is responsible for:

- Developing CLBC specific policies and procedures, where necessary, to support the *Appropriate Use Policy*; and
- Providing support to ensure that supervisors have the information and training necessary to fulfill their responsibilities as set out in this policy.

4.3 Managers Responsibilities

- Managers are responsible for ensuring employees:
 - Are made aware of their responsibilities concerning the appropriate use of Government Information and IT resources;

- Receive the level of training (including privacy, security and records management training) necessary to perform their duties;
- Have access to Confidential Information that is based on the principles of need-to-know, least privilege and for reviewing that access level annually.

Managers must ensure that employees are made aware of their responsibilities concerning the appropriate management of Government Information and IT resources:

- a. At the commencement of their employment;
- b. When a significant change occurs regarding their access to, or authorized use of, Government Information or their use of IT resources, including, but not limited to:
 - i. the issuance of a new Device; and
 - ii. access to a new information database.
- c. When a new or updated version of this directive or similar policy is issued.

Managers must also ensure that employees:

- a. Are familiar with and understand what Confidential Information is and comply with CLBC's IT specific policies and procedures when accessing and managing Confidential Information;
- b. Recognize what Personal Information is and comply with CLBC's privacy policies, in particular, the [Information Incidents including Privacy Breaches Policy](#); and
- b. Have received training appropriate to their position regarding the management of Confidential Information (including privacy, security, and records management training) and what to do if an Information Incident occurs.

4.4 Employees Responsibilities

Employees are responsible for ensuring that the Confidential Information they are working with is protected. This includes, but is not limited to:

- a. Storing Confidential Information in Protected Government and CLBC Systems,
- b. Physically securing Confidential Information in their workspace (e.g. locked drawers or cabinets); and
- c. Limiting the amount of Confidential Information, in particular Personal Information (which is subject to legal restrictions), that is disclosed through email.

REFERENCES

[Confidentiality and Information Sharing Policy](#)
[Information and Communication Technology Agreement](#)
[Information Incidents including Privacy Breaches Policy](#)
[Information Technology Asset Management Policy](#)
[Mobile Device User Agreement](#)
[Mobile Device User Policy](#)
[Organizational Information Security Policy](#)

[Organizational Privacy Policy](#)

[Protection of Information Privacy](#)

[Standards of Conduct for Community Living BC Employees](#)

B.C. GOVERNMENT REFERENCES

[Core Policy and Procedures Manual \(CCPM\), Chapter 12 Information Management and IT Management and Chapter 15 Security](#)

[Electronic Transactions Act](#)

[Freedom of Information and Protection of Privacy Act](#)

[Information Management Act](#)

Policy Number IT5.400	Policy Section Information Technology	Effective Date: November 27, 2023
Title: Adobe Acrobat Pro Software Use Policy		Executive Sponsor: Vice President, Information Technology and Project Services

1. PURPOSE

This policy provides direction for Community Living British Columbia (CLBC) staff on how to use Adobe Acrobat Pro software (Adobe Pro) installed on their workstations and other devices. It also supports staff in understanding their records management responsibilities.

It is to be used, along with the *Adobe Acrobat Pro Software User Agreement*, to support CLBC staff in maintaining the integrity, reliability, and authenticity of CLBC records.

This policy, user agreement, and attached appendices apply to all CLBC staff that create, edit, share, and dispose of information. All staff includes, but is not limited to:

- Regular and temporary staff employed by, working for or on behalf of CLBC;
- Contractors and consultants working for or on behalf of CLBC; and
- All other individuals and groups who have access to CLBC's IT systems, and/or key data or information.

2. POLICY

Operational Context

2.1 Adobe Pro software allows users to edit text and images in PDF documents, convert them to other document formats, and add electronic signatures and password protection. Although these features are user-friendly and promote collaboration, they may negatively impact the reliability and authenticity of original records.

CLBC's Requirements

2.2 Adobe Pro supports CLBC staff in complying with:

- CLBC's *Appropriate Use of Government Information and Technology Policy*, and *Records Retention, Management and Disposal Policy*, and
- B.C. Government's *Information Management Act (IMA)* and *Freedom of Information Privacy Protection Act (FOIPPA)*.

2.3 Adobe Pro must not be used to alter approved or final versions of CLBC records.

2.4 Adobe Pro must not be used to convert CLBC records to an alternate format unless required for business purposes.

2.5 CLBC staff must follow the electronic signature procedures outlined in section 3 of this policy and not modify or tamper with electronic signatures.

2.6 CLBC staff must password protect all documents containing personal information before they are emailed to other CLBC staff or authorized users, such as psychologists and service providers. Refer to *Appendix C: How to Encrypt and Password Protect PDFs* for instructions on how to encrypt and password protect documents.

2.7 Upon receiving access to Adobe Pro, CLBC staff must sign the *Adobe Acrobat Pro Software User Agreement*.

3. PROCEDURES

3.1 CLBC staff use Adobe Pro to create and add a signature to PDF documents. Refer to *Appendix A: How to Create Electronic Signatures* for detailed instructions and refer to *Appendix B: How to Add Electronic Signatures to PDFs* to add your electronic signature to a PDF document.

3.2 CLBC staff use Adobe Pro to encrypt, and password protect PDF documents. Refer to *Appendix C: How to Encrypt and Password Protect PDFs*.

4. REFERENCES

CLBC Policies and Guidelines

[Appropriate Use of Information and Technology Resources Policy](#)

[Documentation and Record Policy: Individual Records](#)

[Documentation and Record Policy: Vendor Records](#)

[Information and Communication Technology Agreement](#)

[Information Technology Password Policy](#)

[Organizational Information Security Policy](#)

[Organizational Privacy Policy](#)

[Privacy Guidelines](#)

[Protection of Information Policy](#)

[Records Retention, Management and Disposal Policy](#)

B.C. Government

[Information Management Act](#)

[Freedom of Information and Protection of Privacy Act](#)

Appendix A: How to Create Electronic Signatures

If you have questions, please contact: CLBCServiceCentre@gov.bc.ca

Follow these steps to create an electronic signature:

Step 1: On a white blank piece of paper, sign the paper.

Step 2: Using your smartphone, take a picture of your signature, making sure you capture only the signature and email it to yourself.

OR

Use a Multifunctional Device/Photocopier in your office to scan your signature, written on blank piece of paper, and email it to your government email.

Step 3: Open your email and save the file to your H:\ drive (remember where you saved it as you will need to find it later).

Step 4: Open the saved file, and ensure the signature is clear.

Step 5: Leave the file with your signature open and use the **Snipping Tool** application (you can find it in the Program list). Select the **New** button to create a new snip.



Step 6: Select the signature using the Snipping Tool, and the selection will appear in the Snipping Tool window. Click on the **Save** button to save the signature.



Appendix B: How to Add Electronic Signatures to PDFs

If you have questions, please contact: CLBCServiceCentre@gov.bc.ca

Follow these steps to add an electronic signature to PDF documents:


Step 1: Open Adobe Acrobat to sign the PDF file.

Step 2: Scroll down to the signature line.

Certification and Approval

The Parties have duly executed this Contract as follows:

CERTIFIED by an authorized representative of Community Living British Columbia on the ____ day of _____, 20____.	APPROVED by an authorized representative of Community Living British Columbia on the ____ day of _____, 20____.
_____ CLBC Representative	_____ CLBC Representative
_____ Print Name:	_____ Print Name:
_____ Print Title:	_____ Print Title:



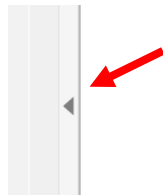
Step 3: If you are using Adobe Acrobat DC (the non-Pro version), select Fill & Sign in the right-side navigation pane.



Note: You cannot scroll down to the signature line after you select Fill & Sign as it will be disabled.

If you are using Adobe Acrobat Pro, the right-side navigation pane will have more options. Select Fill & Sign and ignore all other options.

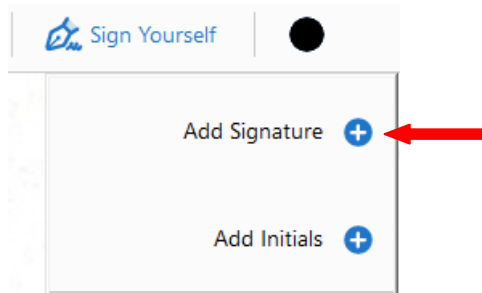
If you cannot view the right navigation pane, select the left pointing arrow to expand the pane.



Step 4: From the top ribbon of your Adobe program, select **Sign Yourself**.

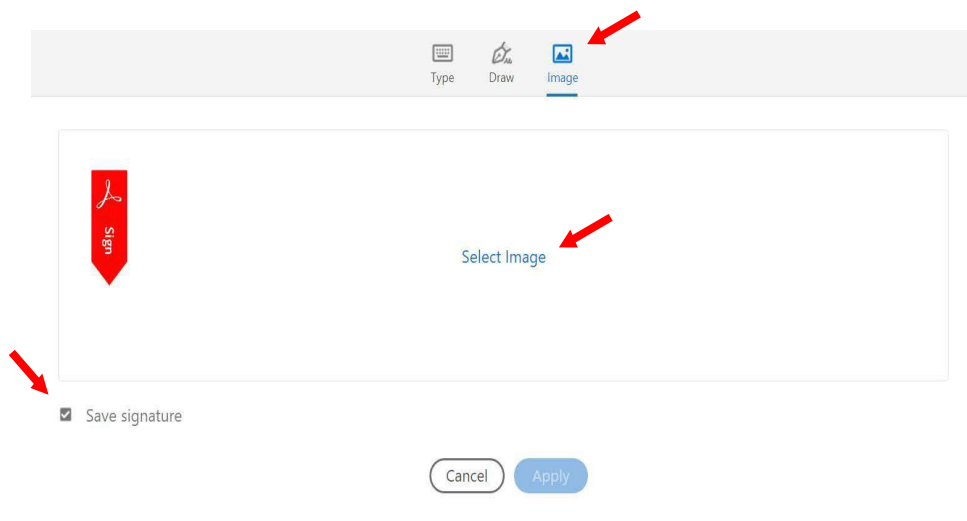


Step 5: From the **Sign Yourself** dropdown menu, select **Add Signature** by selecting the "+" sign.



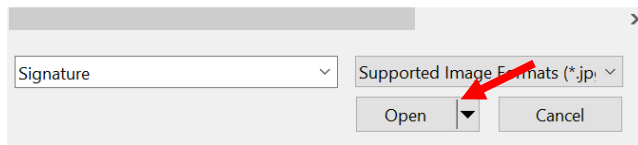
Step 6: Although there are three options available, only select **Image**.

Note: Do not select **Type** or **Draw** as these may be easily duplicated.



Step 7: Ensure there is a check mark next to **Save signature**. If it is not checked, click on it.

Step 8: Click on **Select Image**, find your saved signature on your R drive, and select **Open**.

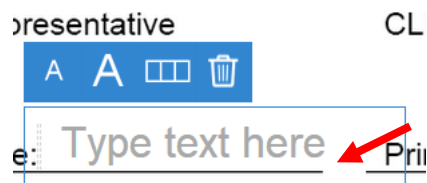


Step 9: After your electronic signature appears, click **Apply**.

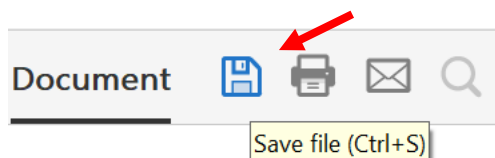
Step 10: If you need to enter dates or print your name, click on the **Ab** icon from the top ribbon.



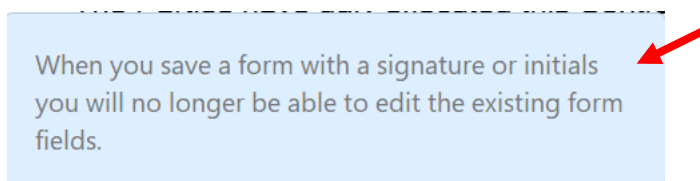
Move your cursor to the line where you wish to enter text, click on the line, and a text box appears. Now, you may type your text.



Step 11: Save your PDF electronically signed document by selecting the Save icon.



After saving the document, a message appears stating you cannot edit the document.



Appendix C: How to Encrypt & Password Protect PDFs

If you have questions, please contact: CLBCServiceCentre@gov.bc.ca

This appendix provides best practices and a quick guide on how to encrypt and password protect PDF documents.

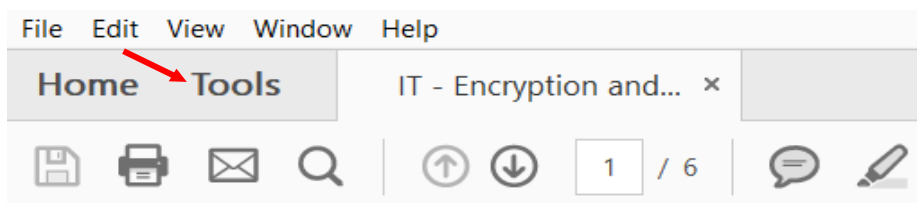
Password Best Practices

1. Documents exchanged through email **must** be password protected as noted in the *Adobe Acrobat Pro Software Use Policy*.
2. The password should be sent in a separate email.
 - a. Do not send the password and the documents in the same email.
 - b. Adjust the subject line to reflect added content (do not use the same subject line as your original email).
 - c. Do not use the word "password" in your subject line.
3. Test the password you have applied to ensure it works before sending it to others.
4. Passwords applied to documents are not recoverable, so if you forget the password, you will need to regenerate the document and re-apply the password.
5. The password should be at least 8 characters, include at least one upper case letter, at least one number, and one special character.
6. Passwords should be unique, **do not** use the same password repeatedly.
7. For further password guidance, refer to the *Information Technology Password Policy*.

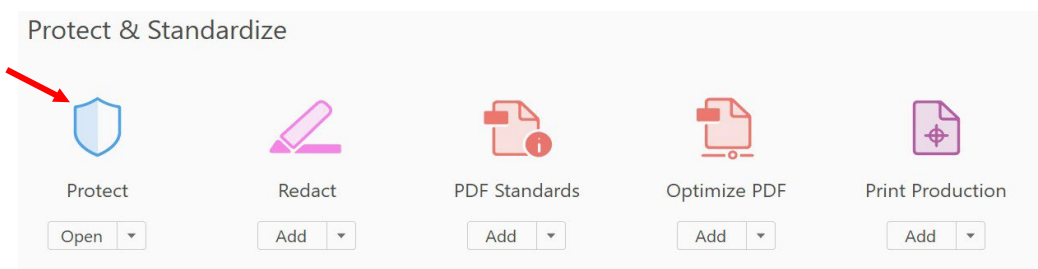
Encrypting and Password Protecting PDF documents using Adobe Pro

Step 1: Open the PDF document.

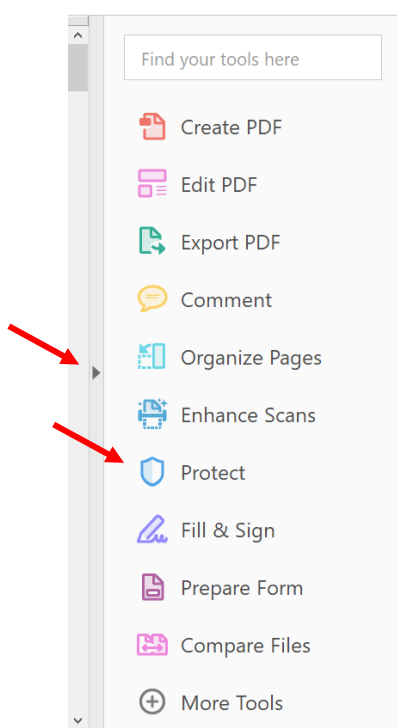
Step 2: From the main toolbar, select the **Tools** tab.



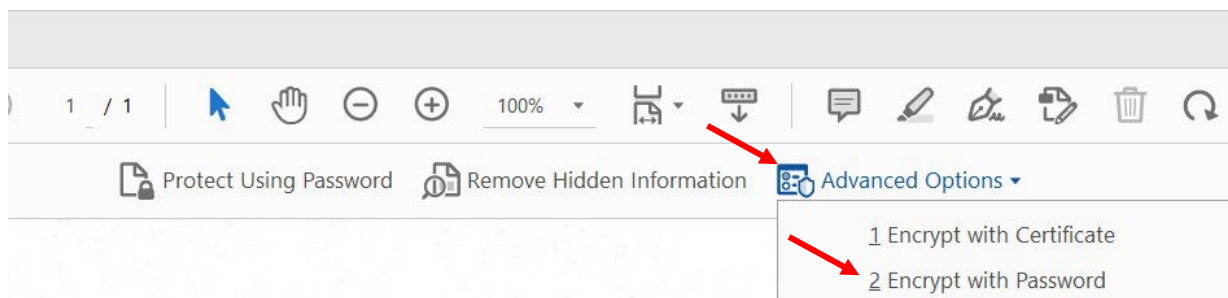
Step 3: Under the **Protect & Standardize** category, scroll down and select **Protect**.



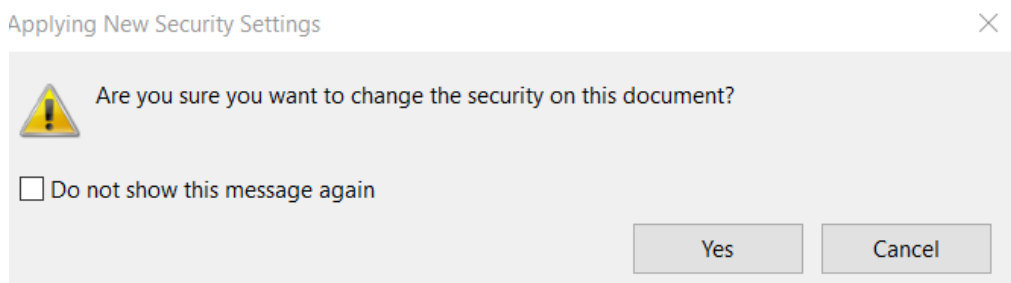
Note: You can also find the **Protect tool** under the tool list in the right-side navigation pane. If you cannot see the navigation pane, click on the arrow next to the sidebar to see it.



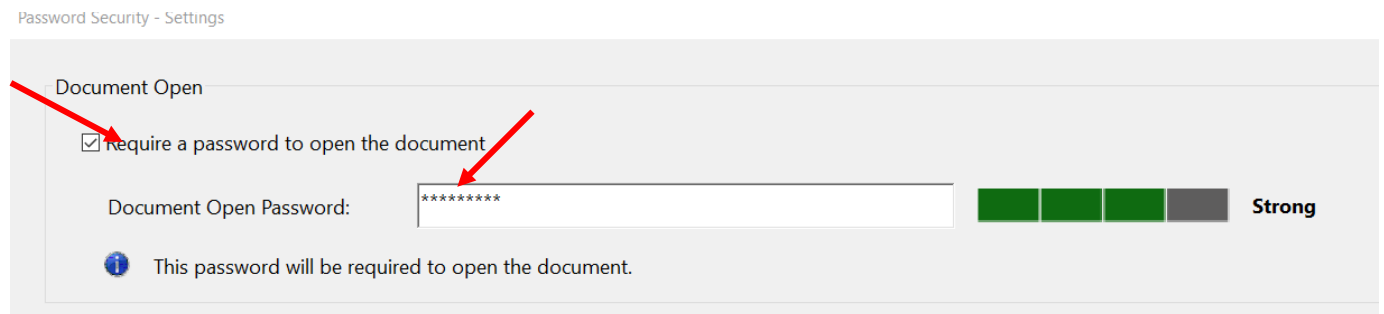
Step 4: The Protect toolbar will now appear at the top of the page. Click on **Advanced Options** and select **2 Encrypt with Password**.



Step 5: When the message below appears on your screen, select **Yes**.



Step 6: Under the **Document Open** section, check **Require a password to open the document**, enter a password, and use the best practices outlined earlier in this document.

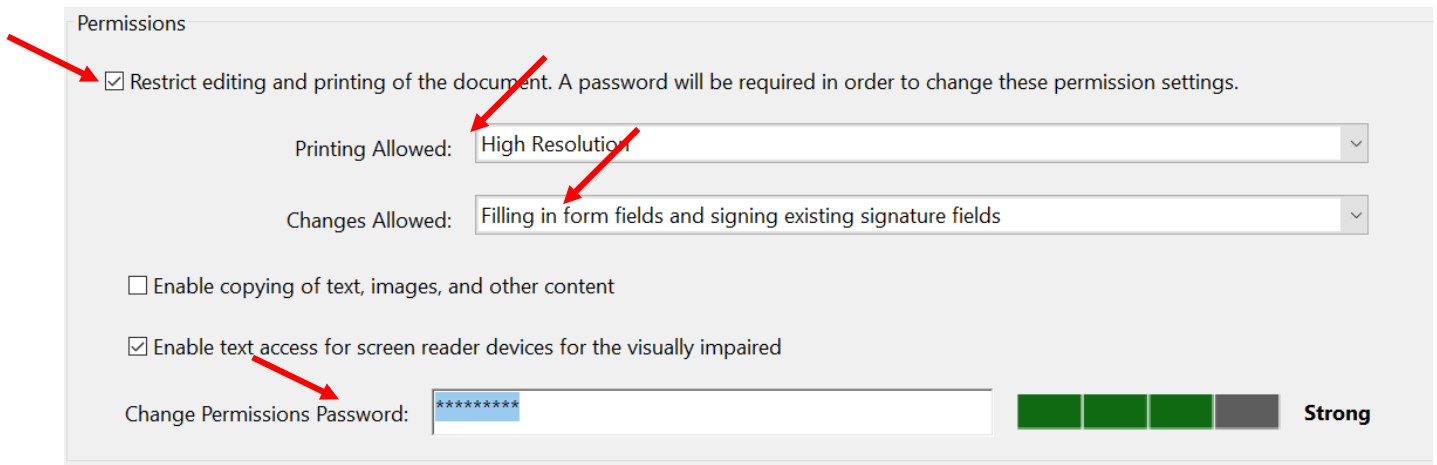


Step 7: Under Permissions, restrict editing and add a second password to limit the access to printing and inclusion of the signature only.

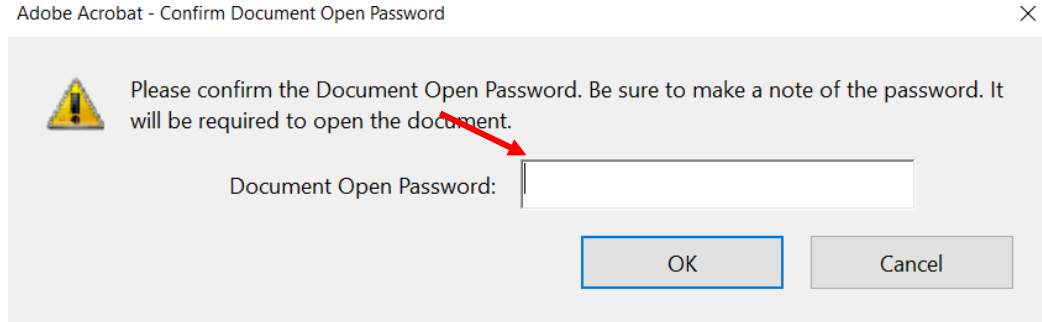
Check **Restrict editing and printing of the document**.

- Under **Printing Allowed**, select the **High-Resolution** option from the dropdown menu.
- Under **Changes Allowed**, select the **Filling in form fields and signing existing signature fields**.

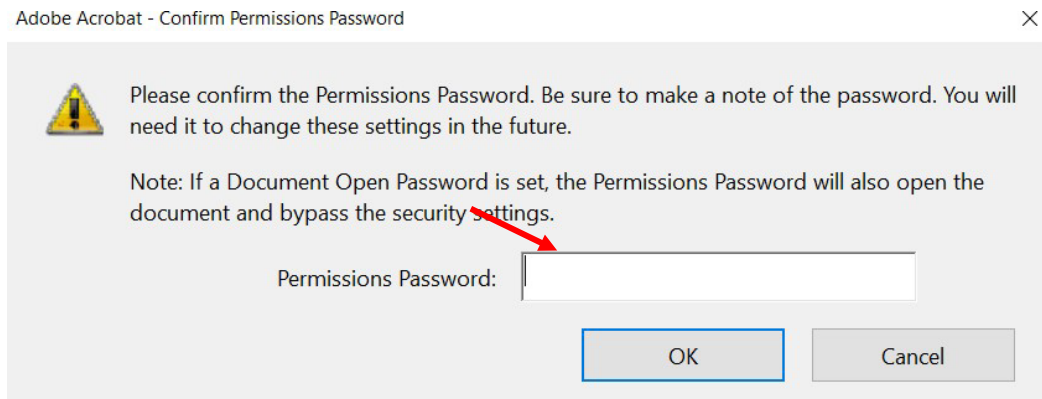
To allow users to make changes to your PDF document, enter another password. It must be different from the first one.



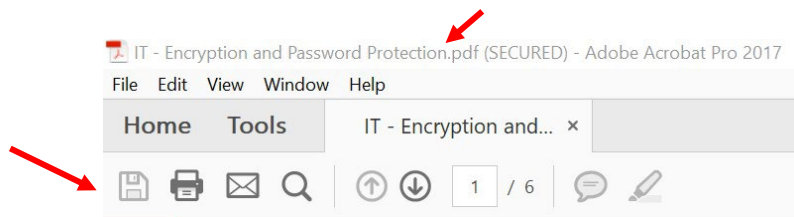
Step 8: Click **OK** and confirm the **Document Open Password** using the first password used at the top of the Document Open section.



Step 9: Click **OK** twice and confirm the **Permissions Password** used under Change Permissions.



Step 10: Click **OK** and save the document using the **Save** button. Note the name of the document will include **(SECURED)** in the title.



Step 11: Close and test your document to ensure it is password protected.

Step 12: If you upload this document to a permanent file on an internal secure drive or SharePoint, remove the password protection so other CLBC staff can access the document.

Adobe Acrobat Pro Software User Agreement

Please email the completed form to: CLBCSDPC@gov.bc.ca

I, the undersigned, have read and agree to follow the terms and conditions outlined in the attached *Adobe Acrobat Pro Software Use Policy*, its appendices, and this agreement. I understand, acknowledge, and agree that:

- If Adobe Pro software is installed on my computer or any CLBC device, I will use it for the intended purposes only.
- I will **not** use the Adobe Pro software for any purpose that is detrimental to CLBC or contrary to client or public interest.
- I will **not** use the Adobe Pro software for any purpose that may affect the integrity, reliability, and authenticity of CLBC records.
- CLBC, in its sole discretion, may uninstall or withdraw my access to Adobe Pro software at any time.

I confirm that I have read and fully understand the attached *Adobe Acrobat Pro Software Pro Software Policy*.

Print Name: _____

Department: _____

Job Title: _____

Signature: _____ Today's Date _____

Please email the completed form to: CLBCSDPC@gov.bc.ca.