Office of the Chief Information Officer Policy Directive

DIRECTIVE:	1/14
SUBJECT:	Appropriate Use of Government Information and Information Technology Resources ("Appropriate Use Policy")
AUTHORITY:	Chapter 12 of the Core Policy and Procedures Manual (CPPM)
EFFECTIVE DATE	March 21, 2014

Purpose:

The purpose of this directive is to set out the policy requirements that all government employees must follow when:

- accessing and managing government information (particularly confidential information); and,
- using information technology (IT) resources.

Additional policies and procedures may be established at the ministry level to support employee compliance with, and monitoring of, this directive and/or to augment this directive with policies and procedures specific to that ministry's information holdings or organizational structure.

Compliance with this directive, and supporting ministry policies and procedures, will ensure that government information is appropriately protected while remaining accessible to those who need it and are authorized to access it. Ultimately, appropriate use of government information and IT resources will ensure that government is able to deliver effective and efficient services to citizens while meeting its statutory obligations to protect information.

Application:

This policy applies to all ministries, agencies, boards and commissions reporting or responsible to the Government of British Columbia.

Advice on this Directive:

Advice on this Directive can be obtained from the:

Strategic Planning and Policy Branch
Office of the Chief Information Officer
Ministry of Technology, Innovation and Citizens' Services

Email: CIOWebCommunications@gov.bc.ca

Version	Date	Changed By	Description of Change
1.0	March 21, 2014	Colleen Rice	
1.1	August 25, 2014	Colleen Rice	Update broken links
1.2	April 21, 2015	Colleen Rice	Update broken links
1.3	September 21, 2015	Colleen Rice	Update broken links
1.4	August 2, 2016	Sherri Kain	Update broken links and contact information

Table of Contents

Definitions:

The following key terms are defined below and appear in bold font throughout the document.

Confidential Information is a category of **Government Information** with confidentiality requirements. It includes, but is not limited to:

- cabinet confidences (for example, a briefing note to Cabinet);
- 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**;
- 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, laptops, tablets, smartphones, and cellphones.

Employee: an individual working for the Government of British Columbia, including **Service Providers** or volunteers.

Government Information: means 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 is a single or a series of unwanted or unexpected events that threaten privacy or information security, including a privacy breach or the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorized by the business owner of that information.

IT Resources: information and communication technologies that include, but are not limited to: information systems, **Devices,** and the government electronic 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: a principle where access is restricted to authorized **Employees** that require it to carry out their work. Employees are not entitled to access merely because of status, rank, or office.

Personal Information: is recorded information about an identifiable individual other than (business) contact information.

Portable Storage Device: is a portable (or removable) device that is primarily designed to store electronic information, for example an external hard drive or a USB flash drive.

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, laptops, tablets, smartphones or other **Devices.**

Record: is anything that is recorded or stored by graphic, electronic, mechanical or other means, including books, documents, maps, drawings, photographs, letters, vouchers, and papers.

Service Provider: means a person retained under contract to perform services for the Government of British Columbia**.**

Roles and Responsibilities:

Deputy Ministers or Equivalent

Deputy Ministers (or equivalent positions) are responsible for ensuring that ministry specific policy and procedures are developed, where necessary, to support the Appropriate Use Policy.

Government Chief Information Officer

The Government Chief Information Officer is responsible for issuing corporate policy, directives and guidelines on the appropriate use of government **IT Resources** and **Government Information.**

Ministry Chief Information Officers or Equivalent

Ministry Chief Information Officers (or equivalent positions) are responsible for developing ministry-specific policies and procedures, where necessary, to support the Appropriate Use Policy.

In addition, Ministry Chief Information Officers are responsible for providing support to supervisors in their respective ministries to ensure that supervisors have the information and training necessary to fulfill their responsibilities as set out in this policy.

Supervisors

Supervisors are responsible for ensuring that **Employees** are made aware of their responsibilities concerning the appropriate use of **Government Information** and government **IT Resources**.

They are also responsible for ensuring that **Employee** access to **Confidential Information** is based on the principles of **Need-to-Know** and **Least Privilege** and for reviewing that access level annually.

They are responsible for ensuring that **Employees** receive the level of training (including privacy, security and records management training) necessary to perform their duties.

In addition, supervisors are responsible for approving the downloading of applications and software by **Employees**. This includes exercising due diligence to ensure that applications and software that are approved for download meet the requirements of this policy.

Further, supervisors are responsible for approving **Employees'** ability to work outside the workplace with **Confidential Information** and ensuring compliance with the Working Outside the Workplace Policy.

Employees

Employees are responsible for complying with this policy and for seeking direction from their supervisors if they have questions regarding this policy.

Policy:

A. General Requirements

1. **Employees** must comply with the Standards of Conduct for Public Service Employees when:

   a) collecting, accessing, using, disclosing or disposing of **Government Information**;
   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. For more information on the use of Social Media, please see the Social Media Guidelines.

2. Supervisors 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 respecting their access to, or authorized use of, **Government Information** or their use of **IT Resources**, including but not limited to:
      i. the issuance 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; and
   d) annually for **Employees** that have access to a significant amount of **Confidential Information**.

3. Supervisors must ensure that **Employees:**

   a) understand what **Confidential Information** is and the ministry policies and procedures that must be followed when accessing and managing **Confidential Information**; and
   b) have received training appropriate to their position respecting the management of **Confidential Information** (including privacy, security and records management training) and what to do if an **Information Incident** occurs.

   For further information on **Information Incidents** please refer to The Information Incident Management Process.

4. Ministry Chief Information Officers (or equivalent positions) must develop ministry-specific policies and procedures, where necessary, to support **Employee** compliance with, and monitoring of, this policy.

5. Deputy Ministers (or equivalent positions) must ensure that ministry-specific policies and procedures are developed, where necessary, to support **Employee** compliance with, and monitoring of, this policy.

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

6. **Employees** must collect, access, use, disclose and dispose of **Government Information** in accordance with policy and law. For example, disposal of information must be done in accordance with approved records schedules, and collection, access, use and disclosure of **Personal Information** must be in accordance with the *Freedom of Information and Protection of Privacy Act* and its supporting policies.

7. Supervisors must authorize an **Employee's** access to **Government Information** based on the principles of "**Need-to-know**" and "**Least Privilege**". Specifically, an **Employee** should have access to the least amount of **Confidential Information** that is necessary to perform their duties.

8. Supervisors must review an **Employee's** level of access to **Confidential Information** at least once per year to ensure that their access level remains necessary and appropriate for the performance of their duties.

9. **Employees** must not collect, access, use, disclose or dispose of **Confidential Information** unless authorized to do so and it is necessary for the performance of their duties.

10. **Employees** must respect intellectual property rights. For example, **Employees** must not use, reproduce, modify or distribute programs or data if they have not received permission from the intellectual property owner to do so.

For more information on intellectual property rights please contact the Intellectual Property Program.

11. **Employees** must store electronic **Records** that relate to government business in **Protected Government Systems**.

    a) In extenuating circumstances, an electronic government **Record** may be temporarily stored outside of a **Protected Government System**, as long as the following conditions are met:

        i. the electronic **Record** is stored on the system or **Device** only as long as is necessary to deal with the extenuating circumstance;
        ii. at the first available opportunity, the **Record** is transferred to a **Protected Government System**; and
        iii. duplicate copies of any electronic **Record** containing **Confidential Information** are deleted from the other system or **Device** as soon as possible.

b) The requirements set out in subsection (a) do not apply to an email **Record** that is automatically stored by government's email system on an **Employee's Device.**

12. **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 Systems**, as set out in section 11, above;
    b) physically securing **Confidential Information** in their workspace (e.g. locked drawers or cabinets);
    c) only disclosing **Confidential Information** to authorized individuals in a secure manner according to ministry approved processes (e.g. **Portable Storage Devices** should only be used in extenuating circumstances when more secure methods are not available and must be encrypted); and
    d) limiting the amount of **Confidential Information**, particularly **Personal Information** (which is subject to legal restrictions), that is disclosed through email.

For further information on encryption standards, please see the Cryptographic Standards for Information Protection.

13. **Employees** may work outside the workplace with **Confidential Information** provided that they have their supervisor's approval and comply with all the provisions of this directive. In addition**, Employees** must:

    a) protect the information, particularly when working in a public environment (for example, ensuring that information is not viewable or accessible by others);
    b) limit the amount of printed materials that are used outside of the workplace (government **Devices** are more secure because they are protected with government security features); and
    c) follow the Working Outside the Workplace Policy.

14 If an **Information Incident** occurs, **Employees** and supervisors must follow the Information Incident Management Process which requires the immediate reporting of any suspected or actual **Information Incident** (including a privacy breach) to the Office of the Government Chief Information Officer and to the Ministry Chief Information Officer.

C. Use and Disposal of Government IT Resources

15. Reasonable personal use of government **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 **IT Resources** or **Government Information**; and
    d) is not used for personal financial gain.

16. For privacy reasons and to reduce the cost of electronic storage for government, **Employees** must limit the amount of personal **Records** they store on government systems.

17. **Employees** must use their government email accounts when conducting government business. This includes while working outside of the workplace.

    In extenuating circumstances, **Employees** may use their personal email or other non-government email, as long as the following conditions are met:

    a) a copy of the email is sent to their government email account, ensuring that the **Government Information** is stored in a **Protected Government System**;
    b) the email is immediately deleted from their personal or non-government email account as soon as possible after dealing with the extenuating circumstance; and
    c) the amount of **Confidential Information** collected, accessed, used or disclosed is limited to the least amount necessary to deal with the extenuating circumstance.

    For information on how to access government email accounts from a remote location, please see the Outlook Web App Guide.

18. **Employees** must not divulge, share or compromise their own or another **Employee's** government authentication credentials (e.g., passwords, access cards, etc.). This includes not divulging passwords to technical support.

19. **Employees** must report any lost or stolen **Device** or access card in accordance with Chapter 20 – Loss Management of the Core Policies and Procedures Manual (CPPM) and Procedure L – Loss Reporting of the CPPM.

20. **Employees** must follow the appropriate policies and procedures when disposing of **IT Resources**. For further information, please see the IT Asset Disposition Site.

D. Access to and Use of Applications and Software

21. **Employees** must have their supervisor's permission, and follow the established procedures, to download or use applications or software from the iStore or the Self-Serve Centre.

22. If an **Employee** wishes to download or use applications or software for government business purposes that are available through the iStore or the Self-Serve Centre and are also available from another source, the **Employee** must download or access the application or software from the iStore or the Self-Serve Centre.

23. **Employees** must not download or use applications or software for government business that are not available from the iStore or the Self-Serve Centre without the permission of their supervisor.

    Applications and software that are not available from the iStore or the Self-Serve Centre may present privacy or security concerns or could impose terms and conditions, such as indemnification clauses, that are unacceptable to government.

24. Supervisors must not permit an **Employee** to download or use applications or software that:

    a) are prohibited by the Government Chief Information Officer;
    b) present unacceptable privacy or security concerns; or
    c) impose unacceptable terms and conditions.

    With respect to section 2(c), supervisors should review their procurement responsibilities in the Core Policy and Procedures Manual - Chapter 6 Procurement before approving an application for download.

E. Monitoring and Investigations

25. Any collection, access, use, transmission, or disposal of **Government Information** or use of government **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, including by engaging in e-discovery;
    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.

26. 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**.

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