Canada

Guideline on Acceptable Network and Device Use

Related Instruments (/pol/doc-eng.aspx?id=27907&section=related)

Supporting Tools

Archives (/pol/doc-eng.aspx?id=27907&section=archives)

Alternate Formats

Complete Text (/pol/doc-eng.aspx?id=27907&section=HTML)

XML (/pol/doc-eng.aspx?id=27907&section=XML)

Expand All | Collapse All

▼ About This Guideline

The *Guideline on Acceptable Network and Device Use* (the Guideline) provides guidance to departmental managers and functional specialists responsible for implementing the *Policy on Acceptable Network and Device Use* (/pol/doc-eng.aspx?id=27122) (the Policy). This guideline is intended for departments to which the Policy applies (see Section 2 of the Policy (/pol/doc-eng.aspx?id=27122&section=text#cha2)). Other Government of Canada institutions are encouraged to follow the advice in this guideline, as appropriate.

This guideline was prepared by the Chief Information Officer Branch of the Treasury Board of Canada Secretariat in consultation with departments and agencies. It replaces those sections of the *Guideline for External Use of Web 2.0* that relate to the use of social media for professional and limited personal use.

▼ 1. Introduction

The widespread adoption of the Internet and the rapid evolution of networks and devices have changed the way public servants work, and have improved the ability to communicate, collaborate, and share information and expertise. For many public servants this advancement has inspired innovative ways of working, including:

- Conducting consultations on new policy instruments through wikis;
- Following and engaging experts and thought leaders on social media platforms;
- Submitting questions or requests through the Internet and social media; and
- Accessing information via smartphones and other user devices.

The Policy requires departments to ensure acceptable and efficient use of Government of Canada electronic networks and devices and to provide open access to Web 2.0 tools and services, in accordance with the *Policy on Government Security* (/pol/doc-eng.aspx?id=16578). This guideline defines professional and personal use of Government of Canada electronic networks, devices and Web 2.0 tools and services. This guideline also provides practical advice and tools that relate to the implementation of the Policy requirements.

Departments are encouraged to consider these best practices when developing their implementation plans.

▼ 2. Defining Professional and Personal Use

In an interactive and mobile work environment, it is important that employees are aware of the expectations of acceptable use when using Government of Canada electronic networks and devices, and Web 2.0 tools and services. This is particularly pertinent given that the networks, devices and social media platforms used for professional purposes are sometimes the same as those used for personal activities, thus potentially blurring the boundaries between the professional and personal use by public servants.

This guideline applies to professional and personal use of Government of Canada electronic networks and devices, and Web 2.0 tools and services by authorized individuals (/pol/doc-eng.aspx?id=27907&section=text#ai), irrespective of location of access. This includes using government-issued devices on government and public networks, as well as using personal devices, if permitted, on Government of Canada networks (e.g., use of a Virtual Private Network on a personal computer).

▼ 2.1 Social Media Activities

Social media and other Web 2.0 tools and services are providing new opportunities for networking and collaborating. There are three key types of use:

"Professional use", which refers to the use of a personal social media account for purposes related to professional activities, such as communicating with professional associations, professional networking (e.g., participating in an online conference), gathering and sharing knowledge (e.g., using Twitter to stay up-to-date on trends or visiting government Facebook pages) and career development (i.e., maintaining a LinkedIn profile).

"Personal use", which refers to the use of a personal social media account for purposes unrelated to professional development or employment (e.g., blogging about gardening tips, checking the weather or bus schedules, or sharing personal or family photos). This type of use is limited and must be conducted on personal time.

A third category is "official use". Only those individuals who have been authorized to represent the Government of Canada can use official social media accounts. Advice on the official use of social media is provided in the *Guideline on Official Use of Social Media* (/pol/doc-eng.aspx?id=27517).

Appendix F (/pol/doc-eng.aspx?id=27907&section=text#appF) provides sample learning tools related to employee use of social media.

Note: Adherence to the behaviours outlined in the *Values and Ethics Code of the Public Sector* (/pol/doc-eng.aspx?id=25049) and departmental codes of conduct is expected for all types of use of electronic networks, devices and Web 2.0 tools and services, including social media. It is important to apply the same judgement to online activities as would apply to similar activities offline. Examples of acceptable and unacceptable use are provided in Appendix B of the Policy (/pol/doc-eng.aspx?id=27122&section=text#appB) and Appendix C of the Policy (/pol/doc-eng.aspx?id=27122&section=text#appC).

▼ 3. Planning for Implementation

The expected results of the Policy are that authorized individuals use Government of Canada electronic networks and devices in an acceptable manner and that they have open access to Web 2.0 tools and services on the appropriate Government of Canada network domains and associated devices. Formulating a course of action to implement the Policy requirements in a timely and effective manner is critical to achieving these outcomes.

A department's approach to planning for implementation will be affected by a number of variables that depend on the department's current state of open access. Departments are encouraged to adapt these recommendations to their own needs.

As a best practice, departments are encouraged to conduct the following activities as part of the planning process:

1. Identify a departmental champion;
2. Conduct a gap analysis;
3. Engage departmental subject matter experts; and
4. Develop an implementation plan.

▼ 3.1 Identifying a Champion

Implementation is the process of turning policy into practice. Executive support can increase the potential for success in implementing the Policy. An effective champion can provide strategic direction to inform the development of an implementation plan and assist in securing the resources needed for implementation. The champion can also be an agent of change.

The Policy requires open access to Internet tools and services, which for some departments will require a culture shift. The presence of an influential leader can help form a new shared value by encouraging others to work differently by promoting the acceptable use of Government of Canada electronic networks and devices, and Web 2.0 tools and services and open access to Internet tools, and by demonstrating change through positive results.

▼ 3.2 Conducting a Gap Analysis

A gap analysis involves determining what steps need to be taken to move from a current state to a target state. Knowledge of expected practices in the target state can help identify actions to close any potential gaps. Departments may wish to frame their gap analyses by using the requirements of the Policy as the future state and determining what gaps exist between the current and future states. Departments can then propose actions to fill the gaps. Highlighting deficiencies will help create the basis of an implementation plan, within which departments can include the resources needed to meet the objectives.

▼ 3.3 Engaging Departmental Subject Matter Experts

Engaging the right people through existing departmental networks or through the creation of a team of experts can support the Policy's implementation goals. It can also demonstrate a more coherent approach to the champion and other executives. It is recommended that departmental representatives be consulted throughout the life cycle of implementation, to ensure that relevant policy and legal considerations are met. Appendix B (/pol/doc-eng.aspx?id=27907&section=text#appB) suggests the departmental experts that could be involved and the value they can add.

▼ 3.4 Developing an Implementation Plan

Developing a formal implementation plan can build a common understanding about what is to be achieved, and the roles and responsibilities of those involved in implementing the Policy. It is a good practice to create an implementation plan in consultation with the members of the team of experts. It is suggested that the plan include the following:

- Purpose;
- Background or Introduction;
- Goals;
- Consultations;
- Roles and Responsibilities;
- Key Tasks;
- Resources;
- Risk Mitigation; and
- Performance Measurement and Evaluation.

An example of an Implementation Plan Template is provided in Appendix C (/pol/doc-eng.aspx?id=27907&section=text#appC).

▼ 4. Implementing the Requirements of the Policy

The objective of the Policy is to ensure acceptable and efficient use of Government of Canada electronic networks and devices, and Web 2.0 tools and services to support enhanced communication and collaboration, thereby improving productivity and program and service delivery to individuals and businesses.

Section 6 of the Policy (/pol/doc-eng.aspx?id=27122&section=text#cha6) states that deputy heads are responsible for ensuring that:

- Effective management and monitoring practices for the acceptable use of Government of Canada electronic networks and devices, and Web 2.0 tools and services are implemented;
- Authorized individuals are informed of the expectations of acceptable use of Government of Canada electronic networks and devices, and Web 2.0 tools and services, departmental monitoring practices and consequences of unacceptable use;
- Open access to the Internet and Web 2.0 tools and services is implemented while meeting the security objectives of the *Policy on Government Security*;
- Learning opportunities regarding the acceptable use of Government of Canada electronic networks and devices and Government of Canada and

external Web 2.0 tools and services are provided to authorized individuals; and
- Reports on the use of Government of Canada networks and devices are made available monthly and as required, to help deputy heads identify, investigate and implement corrective action on issues relating to unacceptable use. See footnote [1] (/pol/doc-eng.aspx?id=27907&section=text#ftn1)

▼ 4.1 Establishing Effective Management and Monitoring Practices

Effective management involves planning, coordinating and monitoring to accomplish desired goals and objectives while using available resources efficiently. Sound operational practices can aid departments in adequately protecting departmental and informational assets and allowing authorized individuals to use networks and devices effectively, efficiently and securely.

As a best practice, departments may want to review existing operational management practices for opportunities to optimize and to validate that the appropriate resources and tools supporting the implementation of the Policy are well coordinated. Finally, ensuring effectiveness of these operating practices through periodic reviews can help ensure ongoing compliance with the Policy.

Examples of best practices are:

- **Establishing monitoring practices:**
  - Defining requirements for regular and special practices for monitoring networks and devices for acceptable use;
  - Communicating monitoring requirements to departmental representatives or Shared Services Canada equivalents responsible for managing network and device monitoring tools; and
  - Coordinating and implementing modifications to monitoring practices as a result of corrective action measures.
- **Managing appropriate and inappropriate use:**
  - Communicating monitoring practices to authorized individuals accessing networks and devices, and any subsequent changes to practices;
  - Receiving, tracking and responding to questions about the Policy;
  - Responding to requests received from management to investigate suspected cases of unacceptable use;
  - Informing the Champion and other executives of compliance with the Policy, including incidents and corrective action measures;
  - Submitting requests for special monitoring to departmental or Shared Services Canada representatives when potential issues of unacceptable use arise;

- Handling confirmed cases of unacceptable use detected by network and device monitoring tools (examples of informal and formal approaches are outlined in Appendix D (/pol/doc-eng.aspx?id=27907&section=text#appD)); and
- Informing departmental security officials if a security incident resulting from unacceptable use is suspected or confirmed.

- **Reporting:**
  - Receiving data on a monthly basis from the various monitoring tools for analysis to ensure compliance with the Policy; and
  - Requesting the generation of unscheduled reports to assist in the investigation of suspected cases of unacceptable use of electronic networks, devices and Web 2.0 tools and services.

▼ 4.2 Informing Authorized Individuals

Communication plays a pivotal role in the successful implementation and application of a policy. Key messages can be developed and communicated using different channels of delivery, ensuring that managers are informed of their responsibilities and that employees are briefed on what is expected of them.

Authorized individuals who use Government of Canada electronic networks and devices, and Web 2.0 tools and services must be informed of expectations for acceptable use, departmental monitoring practices and consequences of unacceptable use. Sample statements for consideration are available in Appendix E (/pol/doc-eng.aspx?id=27907&section=text#appE).

There are several options, both formal and informal, to consider when disseminating required information (Appendix F (/pol/doc-eng.aspx?id=27907&section=text#appF) provides sample learning tools directed to authorized individuals), such as:

- Network login acknowledgements and notifications or security banners (Appendix G (/pol/doc-eng.aspx?id=27907&section=text#appG) provides examples of daily and quarterly network sign-on notifications);
- Departmental electronic newsletters, pamphlets and bulletins;
- Intranets (e.g., Content pages, Frequently Asked Questions (FAQs), wikis and blogs);
- E-mail messages, which can be confirmed by an electronic receipt;
- Streaming video sites (e.g., Transport Canada Social Media at Work YouTube video (http://www.youtube.com/watch?v=JRvY1SzWhl0&list=TLzGuz2cZqZt7ROwwW_GJbyJ3ZRWaYL7aN));
- Topic discussions, lunch and learn sessions, and team meetings;
- Policy and procedures manuals or departmental codes of conduct;

- Orientation of new employees;
- Information posted in common areas (e.g., posters and fact sheets);
- Text included in user account application forms; or
- Terms of use agreements for department-issued devices (e.g., smartphones, external storage devices and tablets), which are signed before taking possession of these devices.

Whether the Policy requirements are being communicated upon the introduction of the new Policy, as part of ongoing awareness, or during periods of amendments to the Policy, it is recommended that departments develop a multi-faceted approach, using as many channels as possible to reach the intended audience.

A best practice is to ensure that relevant information about the Policy is available at all times on the departmental intranet or wiki. By keeping information up to date, departments can adapt messaging to include changes brought about by the introduction of new technologies and Web 2.0 tools and services.

▼ 4.3 Providing Open Access

Open access to Government of Canada electronic networks and devices, including internal and external Web 2.0 tools and services, is essential in transforming the way public servants work and serve Canadians. Open access to an array of Internet-based tools and services (e.g., GCpedia wiki, GCconnex and social networking platforms such as Twitter, YouTube and Facebook) can enhance collaboration and communication.

The information gathered in the gap analysis, outlined in Section 3.2 of this Guideline (/pol/doc-eng.aspx?id=27907&section=text#sec4.2), may have identified the need to provide more open access within the department to meet the Policy requirements. If a strategy is needed to enhance access, the following components could be considered:

4.3.1. Identifying Needs and Aligning with Departmental Priorities

- How are departmental priorities supported by open access?
- Which sites or groups of sites will support authorized individuals' use of the network for government business and for professional development (e.g., social media platforms where the department has an official presence)?
- Are there any responsibilities of specific authorized individuals or groups of authorized individuals that may require access to websites that would normally fall into the category of unacceptable use (e.g., employees

conducting investigation or policy research into an area relating to criminal behaviour)?

4.3.2. Identifying and Overcoming Challenges of Providing Open Access

- What are the perceived or real challenges to providing open access?
  - Information or information technology (IT) security concerns;
  - Network bandwidth;
  - Employee productivity;
  - Access to information and privacy; and
  - Other.
- What are the risk mitigation strategies for these challenges?
  - Use Government of Canada issued devices;
  - Ensure that web browsers and associated applications are up to date and support the functionality of modern websites and tools;
  - Set bandwidth controls, providing reasonable weekly or monthly limits on data use by authorized individuals;
  - Provide warnings to employees if these limits are exceeded;
  - Develop a strategy to acquire more bandwidth capacity as demand for resources continues to grow; and
  - Address employee inefficiency through human resources management processes and consult with human resources to determine the appropriate approach.

Note: See Appendix E of the Policy (/pol/doc-eng.aspx?id=27122&section=text#appE) for additional mitigation measures.

4.3.3. Implementing Open Access

As a baseline, departments could begin by providing default access to social media platforms for which the department has an official account registered, and by limiting access to functionality on those sites that support the objectives of the Policy (e.g., prohibiting access to Facebook games or applications). Departments are also encouraged to document their plans for the incremental expansion of open access once a baseline is established.

In the rare case where business requirements or operational circumstances may dictate the need for restricted access due to security issues, options are available to departments to meet requirements of the Policy. Some options include:

- Providing a standalone unclassified network on which Web 2.0 tools are enabled; or
- Installing kiosk stations or Wi-Fi hotspots that provide open access.

Note: The implementation of an environment supporting open access does not extend to access from classified domains. Connectivity of the classified domains continues to be regulated under existing policy and standards on government security, as well as lead security agency and departmental direction.

It is suggested that departments provide a process for authorized individuals to request access to new websites or online tools, which can be considered in future plans to expand access, given security considerations.

4.3.4. Reviewing and Evaluating Open Access Practices

Departments are encouraged to review their open access practices on an annual basis to assess progress and to address issues that arise regarding changes in policy or emerging technologies. This will also ensure that open access is being provided in accordance with the *Policy on Government Security*. Appendix E of the Policy provides guidance on security measures to support the implementation of the Policy and to protect Government of Canada networks, devices and information.

▼ 4.4 Providing Learning Opportunities for Authorized Individuals

In general, risks associated with unacceptable use, security incidents, and privacy breaches can be minimized through the provision of effective learning opportunities supported by an effective monitoring capability. Learning activities can reinforce the role of managers and authorized individuals in ensuring good practices and compliance with policy requirements.

When generating awareness about the Policy, departments may want to inform managers and supervisors of the implications of the new Policy in advance. Their role can help ensure compliance with the Policy, thereby assuring the operational effectiveness and integrity of the department. This can also better equip management and supervisors to respond to questions from employees.

Consideration may also be given to linking key messages about expected behaviours when using Government of Canada networks, devices and Web 2.0 tools to the *Values and Ethics Code for the Public Sector (/pol/doc-eng.aspx?id=25049)* and the departmental code of conduct. It may be important to reinforce that the same rules regarding upholding the values of the public sector apply both online and offline.

Learning opportunities may include, but are not limited to:

- Information sessions (e.g., online or in-person);
- Orientation sessions for new employees, including discussions on acceptable and unacceptable use of networks and devices;

- Canada School of Public Service and the Communications Security Establishment IT Security Learning Centre course offerings;
- Regular discussions between managers and their staff;
- Online learning products, including self-assessment tests and YouTube videos;
- Presentations at branch-level town halls, meetings or workshops;
- Communications products that can be distributed to authorized individuals or posted in prominent locations in the workspace (Appendix F (/pol/doc-eng.aspx?id=27907&section=text#appF) provides sample communication tools);
- Communities of practice discussions, either in-person or via internal Government of Canada online collaborative tools;
- Mentoring programs, especially when helping employees transition to the use of Web 2.0 tools as part of their work; and
- Leveraging existing activities (e.g., Security Awareness Week) to communicate key messages about the Policy.

Ongoing learning opportunities allow departments to update information as Internet-based tools continue to evolve, and can be supplemented with examples that represent the department's individual circumstances. It is recommended that the definitions (in Appendix A (/pol/doc-eng.aspx?id=27907&section=text#appA)) and the lists of non-exhaustive examples of acceptable and unacceptable use, as described in Appendix B of the Policy (/pol/doc-eng.aspx?id=27122&section=text#appB) and Appendix C of the Policy (/pol/doc-eng.aspx?id=27122&section=text#appC), be considered when developing learning materials. Appendix F provides sample learning tools.

▼ 4.5 Monitoring Networks and Reporting

Having the appropriate tools and processes in place to identify and investigate suspected cases of unacceptable use can support the accountability of deputy heads to address Policy non-compliance in an effective and organized manner.

Data from network monitoring tools supply some of the evidence needed to recognize and confirm incidents of unacceptable use. The Policy requires that regular monthly, and as required, reports be provided based on this data to assist departments in the identification, investigation, and implementation of corrective action pertaining to unacceptable use. Where network services are supplied by Shared Services Canada, the responsibility for providing these reports lies with the deputy head of Shared Services Canada. For those departments not served by Shared Services Canada, the responsibility to meet this requirement resides with the individual department.

Following the validation of the initial implementation of the Policy requirement regarding monitoring and reporting, departments may consider liaising regularly with Shared Services Canada or the departmental equivalent to ensure that monitoring tools are configured to generate the data needed to assess the acceptable use of networks and devices.

Unacceptable use can range from minor to very serious issues. Developing a Corrective Action Plan in advance to address incidents of unacceptable use can assist the deputy head in resolving matters of non-compliance efficiently and consistently. Appendix D (/pol/doc-eng.aspx?id=27907&section=text#appD) provides a list of key elements and suggested options for remedial action that could be included in a Corrective Action Plan.

▼ 5. Enquiries

For questions on this guideline, please contact TBS Public Enquiries (/contact/contact-eng.aspx).

▼ Appendix A: Definitions

Acceptable use

Permitted use of Government of Canada electronic networks and devices by authorized individuals:

- To perform activities as a part of their official duties;
- For career development and other professional activities; and
- For limited personal use that is conducted on personal time; that is not for financial gain; that does not incur any additional costs for the department; and that does not interfere with the conduct of business.

All use of Government of Canada electronic networks and devices must be in compliance with the Values and Ethics Code for the Public Sector and all other related Treasury Board policies and departmental codes of conduct and policies. Use of Government of Canada electronic networks and devices must not give rise to a real, potential or apparent conflict of interest or in any way undermine the integrity of the department. (See also Appendix B of the Policy (/pol/doc-eng.aspx?id=27122&section=text#appB))

Access

Gaining entry to an electronic network that the federal government has provided to Government of Canada authorized individuals. Access to such electronic networks may be from inside or outside government premises. Access may support telework and remote access situations, or situations where authorized individuals are using electronic networks provided by the federal government on their own time for limited personal use.

Authorized individuals

Individuals working with the Government of Canada, including employees of the federal government as well as casuals, contractors, students and other persons who have been authorized by the deputy head to access Government of Canada electronic networks and devices.

Electronic network

Groups of computers and computer systems that can communicate with each other, including without limitation, the Internet, Government of Canada electronic data networks, voice and video network infrastructure, and public and private networks external to a department. The network includes both wired and wireless components.

Internet

A global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP (Transmission Control Protocol and Internet Protocol)) to serve users worldwide.

Learning opportunities

Diverse learning methods or tools, formal or informal, to generate awareness or acquire knowledge about the acceptable use of Government of Canada electronic networks and devices and Government of Canada and external Web 2.0 tools and services. These approaches can include, but are not limited to, information or orientation sessions, YouTube video, information provided on departmental intranet sites, manager debriefs, account sign-on notifications and electronic newsletters.

Monitoring practices

Use of a software system that monitors an electronic network for slow or failing components, and notifies the network administrator in cases of outages, and that can monitor the network activity of specific individuals for which there is suspicion of unacceptable network usage. Recording and analysis of the use of electronic networks are used for operational purposes and for assessing compliance with government policy.

Regular monitoring

Includes practices conducted in the course of operations within a department. These practices can include operational analysis of logs indicating the Internet sites visited by authorized individuals, the files downloaded or uploaded, and the key-word searches of files on Government of Canada network servers or user devices accessing the network.

Special monitoring

May be used when unacceptable use is suspected because of anomalies found in network usage patterns; logged attempts to access restricted areas on the network or sites that are unacceptable or deemed a legitimate IT security threat to the network; or reports of possible unacceptable use.

Open access

Refers to the provision of Internet access, in accordance with the Policy on Government Security, to authorized individuals via Government of Canada electronic networks and devices that, from the perspective of firewall settings, is substantively equivalent irrespective of department or access medium. Internet sites that enhance productivity, communication and collaboration are not blocked with the exception of those that present a legitimate IT security threat and where content substantively falls into the category of unacceptable use.

Unacceptable use

Any activity that violates Treasury Board or departmental policy instruments or other published requirements, including, but not limited to, activity or behavior that:

- May give rise to criminal offences;
- Violates federal and provincial statutes;
- Impacts negatively on the performance of Government of Canada electronic networks and devices;
- Impedes departmental operations or the delivery of services;
- Breaches the Duty of Loyalty requirement for public servants (i.e., does not refrain from public criticism of the Government of Canada); and
- Could be deemed to reasonably result in civil lawsuits. (See also Appendix C of the Policy (/pol/doc-eng.aspx?id=27122&section=text#appC)

User devices

Physical devices found or brought into the work environment that are used by authorized individuals to access Government of Canada electronic networks and databases. The physical devices can include, but are not limited to, the following: desktop workstations, laptops, notebooks, tablets, smartphones, cellphones, peripherals such as printers and scanners, memory devices such as USB

(Universal Serial Bus) flash drives, CD (Compact Disc) drives and DVD (Digital Versatile Disc) drives, webcams and any other computer hardware used to obtain, store or send information.

Web 2.0

Includes Internet-based tools and services that allow for participatory multi-way information sharing, dialogue, syndication, and user-generated content. This can include social media and collaborative technologies.

▼ Appendix B: Consulting Departmental Subject Matter Experts

The following is a list of departmental subject matter experts to engage when implementing the *Policy on Acceptable Network and Device Use* (the Policy) and developing Corrective Action Plans. Consultations with these specialists can confirm a sound management approach to implementation and ensure that related legislation and policy requirements are being respected.

Subject Matter Experts	Reasons To Consult
Access to Information and Privacy	• Ensures that privacy concerns are considered; • Confirms that the operational processes and procedures needed to implement the Policy requirements are compliant with the Access to Information and Privacy (ATIP (Access to Information and Privacy)) legal and policy framework; and • Provides expert advice when investigating potential cases of unacceptable use and Policy non-compliance.
Communications	• Provides strategic communications advice for the creation of key messages and materials conveying the Policy oversight responsibilities of management and the expected behaviour of authorized individuals when using departmental networks and devices, and Web 2.0 tools and services; • Assists in the development and review of key messages for managers to support a consistent approach to communicating the Policy requirements that authorized individuals can understand and can act upon; and • Identifies opportunities in the department's communications calendar for promoting Policy awareness (e.g., intranet spotlights or articles in the departmental newsletter).
Human Resources	• Assists in the development or review of the Corrective Action Plan to ensure that proposed resolutions (informal and formal) address cases of unacceptable use; and • Assists on a case-by-case basis on known cases of unacceptable use.

Information Management	• Validates business needs and determines how appropriate information management practices can be incorporated into operational processes relating to the implementation of the Policy (e.g., what and why information needs to be collected and who needs access to it and for how long); and • Checks proposed retention and disposition schedules of data supporting the identification, investigation and corrective action of non-compliance with the Policy (e.g., monitoring data, reports, and documentation linked to investigations of unacceptable use).
Security	• Provides expert advice when investigating potential cases of unacceptable use and policy breaches from both an IT Security and the corporate security perspective; • Ensures that effective management and monitoring practices supporting the implementation of the Policy comply with the *Policy on Government Security*; • Ensures that IT Security and corporate security concerns are considered (i.e., an understanding of the risks, potential threats and necessary mitigation measures in order to support the policy). See Appendix E of the *Policy on Acceptable Network and Device Use* for security consideration best practices; • Ensures that the departmental network security authorizations consider and include the operation of Web 2.0 tools and open access; • Provides endorsement that the operational processes and procedures needed to implement Policy requirements are compliant with the Security of Information Act (http://laws-lois.justice.gc.ca/eng/acts/O-5/); • Confirms the appropriate security clearance for individuals granted access rights to information gathered through regular and special monitoring of networks and devices; and • Identifies opportunities to generate awareness about the Policy through departmental security awareness initiatives (e.g., Security Awareness Week, departmental security training and awareness programs).
Legal Services	• Confirms that the management approach and the proposed operational processes and procedures supporting implementation of the Policy respect related laws and regulations; • Advices on privacy considerations relating to regular and special monitoring practices; and • Reviews network sign-on and other electronic and paper-based notifications used to inform authorized individuals of expectations of acceptable use, monitoring practices and consequences of unacceptable use.
	• Examines the communication materials used to inform authorized individuals of expectations of acceptable use of networks, devices, and social media to ensure alignment

Values and Ethics	with the *Values and Ethics Code for the Public Sector* and the departmental code of conduct; • Answers questions about the linkage between conflict of interest and wrongdoing in the workplace, and appropriate and inappropriate use of electronic networks, devices and Web 2.0 tools and services; and • Identifies opportunities to raise awareness about the Policy during corporate awareness activities on values and ethics.

A continuing liaison with subject matter experts during implementation and beyond is considered a best practice to support monitoring of policy compliance. In addition to consulting internally, gathering best practices and lessons learned from colleagues external to the department may also yield concrete benefits. Engaging horizontally can identify solutions to implementation challenges, identify efficiencies by avoiding duplication of effort and encourage a more consistent implementation approach across the Government of Canada. This can be accomplished by consulting established networks and by leveraging the knowledge and expertise of active interdepartmental corporate service communities on GCpedia and GCforums (e.g., ATIP (Access to Information and Privacy), Human Resources, Information Management, Internal Services, IT Security and the Security Awareness Working Group).

▼ Appendix C: Sample Implementation Plan Template

This appendix provides a sample implementation plan template for the *Policy on Acceptable Network and Device Use* (the Policy). It is recommended that departments adapt this tool and others in this Guideline for their own needs based on their current state of open access. A good practice is to include all subject matter experts in the creation of the implementation plan to ensure that other policy considerations will be addressed in the plan.

Sample Implementation Plan Template

1.0 Document Title

[Department Name] Plan to Implement the Policy on Acceptable Network and Device Use.

2.0 Purpose

This section states the goal(s) and objectives of the plan (i.e., what is to be achieved).

3.0 Background or Introduction

This section provides an overview of the work to be done as well as appropriate information about the requirements and the approach to implement the Policy.

4.0 Consultations

This section identifies subject matter experts who have been consulted during the creation of the implementation plan and outlines the rationale for including them in the process.

5.0 Roles and Responsibilities

This section identifies the name of the responsible individual or functional team leading and coordinating the implementation, and the departmental areas that will be responsible for key functions. It also outlines the roles and responsibilities of those who will be involved in completing the tasks needed to implement the Policy.

6.0 Scheduled Tasks

This section lists the tasks to be implemented chronologically, the individual or group responsible and the timeline for completion. It is recommended to include beginning and end dates for each task.

7.0 Resources

This section proposes the various resources needed to implement the plan (e.g., human, financial, and software). It may also include the training necessary for personnel implementing the plan.

8.0 Risk Mitigation

This section describes the options and actions to reduce the risks that may pose a threat to the implementation of the plan. The risks and mitigation strategies may be identified through a separate risk management process (i.e., Harmonized Threat and Risk Assessment and Security Assessment and Authorizations).

9.0 Measuring Performance and Evaluation

This section describes the approach to measuring the success of the implementation. It states how success will be defined and what data will be used to report on implementation results.

▼ Appendix D: Corrective Action Plans and Options for Remedial Action

This section lists remedial solutions and suggests that remedial action is taken on a case-by-case basis. A Corrective Action Plan is a series of steps that are undertaken to address non-compliance and prevent its reoccurrence. Remedial action does not always have to be reactive; preplanning can potentially reduce the response time and increase the ability to handle issues in a timely manner.

It is conceivable that options for addressing different cases of unacceptable use may be available, depending on the severity of the situation. Incidents of unacceptable use may be easily identified, contained or eliminated through immediate corrective action, while others may require a longer period of review to confirm the non-compliance, and to propose and implement a resolution. In either situation, it is recommended that departments be proactive in developing a Corrective Action Plan with options for remedial action to ensure that instances of unacceptable use are handled effectively and efficiently.

▼ Corrective Action Plan

The details of a Corrective Action Plan will depend on departmental needs; however, the plan does not have to be overly complex to be practical. Some elements of a Corrective Action Plan could include, but are not limited to, the following:

Sample Corrective Action Plan Template

1.0 Document Title

Corrective Action Plan for Incidents of Non-Compliance With the "Policy on Acceptable Network and Device Use".

2.0 Purpose

This section states the goal(s) and objectives of the plan (i.e., what is to be achieved).

3.0 Background or Introduction

This section provides an overview of the corrective action process as well as high-level information about the requirements and the approach to implementing corrective action in suspected cases of non-compliance with the Policy.

4.0 Corrective Action Plan Process

This section outlines all actions needed to identify, investigate and resolve any deficiencies in meeting Policy requirements.

5.0 Schedule of Activities

This section maps the activities to a schedule, including target completion timelines for actions to alleviate immediate risks and in some cases, for preventive measures to curtail the threat of reoccurrence.

6.0 Resources

This section proposes the various resources needed to implement the plan (e.g., human, financial, and software). This section highlights:

- The position responsible for monitoring and maintaining the corrective action process;
- Positions or functional units responsible for implementing the corrective action activities;
- Information needed to identify and investigate suspected cases of unacceptable use; and
- Special equipment, software or services (e.g., management of network monitoring software and reports supplied by departmental functional specialists or Shared Services Canada equivalents) needed to execute the plan.

7.0 Training and Learning Opportunities

This section identifies any special training needed to execute the plan for:

- Individuals implicated in the corrective action process, including notifications and guidance on procedural updates; and
- Managers and their role in executing the corrective action activities.

It also identifies any new materials needed for management or authorized users of the network to reduce the risk of reoccurrence.

8.0 Corrective Action Scenarios

This section lists types of non-compliance and outlines corresponding remedial solutions. It also provides information about the resources and timelines associated with the corrective action, including, but not limited to:

- Type of non-compliance (e.g., excessive use of bandwidth, disproportionate use of social media unrelated to work-related duties, or disclosure of sensitive information);
- Type of corrective action to be taken and how it will be implemented;
- Date of completion (e.g., duration, including start and end dates);
- Individual or functional unit responsible for implementation;
- Steps to validate the implementation of the corrective action; and

- Position responsible for verifying the effectiveness of the remedial action.

Note: This approach could also be used for reporting to the champion and other executives on the status of issues related to non-compliance.

9.0 Communication

This section describes who needs to be notified of non-compliance and the work being undertaken to rectify the problem. It also defines from whom the approval is required and how it will be obtained (only if approvals are required) to proceed with certain corrective action measures.

10.0 Performance Monitoring and Evaluation

This section summarizes how the department will monitor the effectiveness of the plan throughout implementation to determine whether the plan achieves the intended goals. It will also validate the corrective action process and determine whether improvements are required.

11.0 Reporting

This section outlines the information to be included in the management report and the frequency with which the Champion and other executives will be informed of issues of non-compliance with the Policy, including any incidents and corresponding resolutions to mitigate future risks.

▼ Options for Remedial Action

Triggers initiating a corrective action process can be determined by analyzing network performance reports linked to data about unacceptable use or by investigating a complaint of unacceptable use received by a manager or another employee. This can lead to informal and more formal remedial action to address issues of non-compliance, depending on the seriousness of the problem.

In less severe cases, departments may want to consider a more informal approach to address non-compliance. For example, excessive bandwidth use could trigger a system-generated message to confirm whether Policy non-compliance is linked to a legitimate work-related activity or to address a minor non-malicious breach of the Policy without formal action being taken. The preliminary notification can also be used as an awareness opportunity to restate departmental bandwidth usage limits.

Processes for repeated unacceptable use may include secondary or subsequent e-mail warnings to the authorized user, his or her immediate supervisor, the branch executive and human resources to rectify the issue. As a

best practice a progressive approach is recommended, such as the following:

- The first notification is sent to the authorized individual to confirm unacceptable use, to remind the recipient of the Policy requirements and how to avoid the unacceptable behaviour in the future;
- The second notification is sent to the authorized individual and his or her manager;
- The third notification is sent to the authorized individual, his or her manager, the branch executive and human resources, for further follow-up.

More formal methods of corrective action could be applied upon repeated minor abuses of Government of Canada networks and devices by those who have been previously warned of their unacceptable use or when serious cases of unacceptable use have been confirmed. These corrective actions can include an oral or a written reprimand, revocation or limitation of network access, or suspension or termination of employment. It may be required that each case of unacceptable use be assessed on an individual basis and reviewed by the relevant departmental subject matter experts noted in Appendix B (/pol/doc-eng.aspx?id=27907&section=text#appB). These actions would be independent of any criminal or civil proceeding against an authorized individual.

Note: It is good practice to conduct a review of the proposed Corrective Action Plan with appropriate departmental experts (refer to Appendix B (/pol/doc-eng.aspx?id=27907&section=text#appB)) to ensure that privacy, security and information management requirements are considered.

▼ Appendix E: Sample Communications Statements

This appendix provides sample statements that can be used to communicate the expectations of acceptable use, departmental monitoring practices and consequences of unacceptable use to authorized individuals who use Government of Canada electronic networks and devices, and Web 2.0 tools and services.

These sample statements can be adapted and tailored by departments as needed. Before using these statements, it is recommended that they be reviewed by the departmental subject matter experts identified in Appendix B (/pol/doc-eng.aspx?id=27907&section=text#appB) of this guideline, to ensure consistency with other policies (e.g., human resources, privacy and security) and other departmental requirements.

▼ Expectations of Acceptable Use

- By using Government of Canada electronic networks and devices, authorized individuals agree to the terms and conditions set out by legislation, and relevant Treasury Board policies and departmental documentation governing the use of Government of Canada electronic networks and devices.
- Authorized users of Government of Canada electronic networks and devices are expected to:
    - Use Government of Canada electronic networks and devices in a responsible and informed way;
    - Understand the obligations of expected behaviour outlined in the *Values and Ethics Code for the Public Sector* and the departmental code of conduct, which apply at all times when using Government of Canada and external Web 2.0 tools and services;
    - Take precautions to protect electronic network and device passwords and accounts from unauthorized access and other misuse;
    - Contact management when in doubt about proper usage procedures and practices; and
    - Inform departmental security officials immediately of any suspected security incidents related to the use of electronic networks and devices.

Note: Examples of acceptable and unacceptable use in Appendix B of the Policy (/pol/doc-eng.aspx?id=27122&section=text#appB) and Appendix C of the Policy (/pol/doc-eng.aspx?id=27122&section=text#appC) can also support an understanding of expectations.

▼ Monitoring Practices

- The network is restricted to authorized individuals only and the department reserves the right to monitor network activity. All blocking and monitoring will be done in compliance with the *Privacy Act* (http://laws-lois.justice.gc.ca/eng/acts/P-21/) and the *Canadian Charter of Rights and Freedoms* (http://laws-lois.justice.gc.ca/eng/Const/page-15.html#h-39).
- Electronic network and device monitoring is conducted for work-related purposes (e.g., assessing system or network performance, protecting government resources or ensuring compliance with Treasury Board and departmental policies and codes of conduct.
- All information transmitted and stored on Government of Canada networks and devices, whether professional or personal in nature, may be accessible under the *Access to Information Act* (http://laws-lois.justice.gc.ca/eng/acts/A-1/) and the *Privacy Act*, subject to exclusions and exemptions under these Acts.

- Special monitoring may be permitted without notice in instances when investigating potential cases of unacceptable use.
- Special monitoring may include using any of the regular monitoring practices of the organization in a user-specific manner to find relevant information. It may also include additional investigation, such as, reading the contents of individual e-mail, hard drives, shared drives, document management systems, USB (Universal Serial Bus) drives, or other Government of Canada-provided electronic network or storage systems.

Note: It is recommended that regular monitoring practices be communicated in a privacy notice, as outlined in Appendix D of the Policy on Acceptable Network and Device Use.

▼ Consequences of Unacceptable Use

- Disciplinary measures or sanctions may be taken as deemed appropriate as a result of unacceptable use of electronic networks or devices by authorized individuals.
- The measures taken will be assessed on a case-by-case basis, and may include:
  - Oral or written reprimand;
  - Revocation or limitation of network access;
  - Revocation of security clearance; or
  - Suspension or termination of employment.
- Disciplinary action shall be independent of any criminal or civil proceeding against an authorized individual.

Note: Further information and guidance regarding disciplinary measures can be found in the *Framework for the Management of Compliance* (/pol/doc-eng.aspx?id=17151) and the *Guidelines for Discipline* (/pol/doc-eng.aspx?id=22370).

▼ Appendix F: Sample Learning Tools

Various tools may be used to support the development of materials to generate awareness of the requirements of the *Policy on Acceptable Network and Device Use* (the Policy) for authorized individuals using Government of Canada networks and devices. The topics of communication include:

- 1. Employee Use of Social Media;
- 2. Frequently Asked Questions Regarding the *Policy on Acceptable Network and Device Use*;
- 3. Use of External Storage Devices;

- 4. Security Reminder Bulletin; and
- 5. Smartphone Etiquette.

▼ 1. Employee Use of Social Media

Types of Social Media Use:

Official use:

Using an official social media account for Government of Canada purposes such as communication, service delivery, collaboration and other purposes within the scope of a department's mandate, including as a designated spokesperson for the department.

Professional use:

Using a personal social media account for purposes related to professional activities, including professional associations and networking (e.g., participating in an online conference), knowledge gathering or sharing (e.g., using Twitter to stay up-to-date on trends; visiting government Facebook pages), and career development (e.g., maintaining a LinkedIn profile).

Personal use:

Using a personal social media account for purposes unrelated to professional development or employment (e.g., blogging about gardening tips; sharing family photos).

Social media and other Web 2.0 tools and services are rapidly changing the personal and professional lives of public servants. Opportunities that now exist for networking and collaborating on a global scale were unthinkable a generation ago. The majority of Canadians now use social media on a regular basis and employees of the Government of Canada are no exception.

As the citizens, communities and clients served by government increase their use of Web 2.0 tools and services to organize, share, and interact, government employees are becoming more active in these online spaces in their roles as public servants. Whether using a wiki to develop a new policy instrument collaboratively, following and engaging with experts and thought-leaders on Twitter, or managing an official departmental Facebook page to answer questions from citizens, Web 2.0 tools and services are becoming a larger part of our professional lives. These same Web 2.0 tools and services are often used in our personal lives, blurring the boundaries between online interactions as public servants and as private citizens. As the *Prime Minister's Advisory Committee on the Public Service* (http://www.clerk.gc.ca/eng/feature.asp?pageId=297) noted, "These tools are transformative and unstoppable and the Public Service must take full advantage of these new ways of working."

What is Web 2.0?

"Web 2.0" is a broad term that refers to Internet-based tools and services that allow for participatory, multi-way information sharing, as opposed to earlier uses of the web that were primarily characterized by one-directional publishing of information. The term "Web 2.0" is often used interchangeably with "social media," and includes popular platforms such as Twitter, Facebook, and YouTube, or blogging platforms like Tumblr. These platforms allow participants to have a distinct user profile which they use to create and share user-generated content such as text, pictures or videos, and to facilitate community interaction. "Web 2.0" can also include technologies such as wikis or Google Docs, which allow multiple users to create and edit content collaboratively.

These new online collaboration tools offer tremendous benefits. However, in an era of instant global communications, it is important to consider the special responsibilities that we have as employees of the Government of Canada, including for the use of Government of Canada networks and devices. The public service has a long and proud tradition of providing impartial advice to the government of the day. This is derived from the importance and necessity of an impartial and effective public service to achieve its mission of helping the duly elected government, under law, to serve the public interest.

The *Policy on Acceptable Network and Device Use* applies whenever using a Government of Canada network or a Government of Canada-issued device, including a work computer while at the office, a work device (e.g., a Government of Canada laptop or smartphone) on a home network, or a work or personal device to remotely access a government network. When using the Internet, social media and other Web 2.0 tools and services, it is important that Government of Canada employees consider the context of online activities and apply the same judgement that they would to a similar activity in the offline world.

Want to learn more about acceptable use of social media?

For an engaging overview of important points to keep in mind as an employee using social media, take a look at the online video "Social Media at Work", developed by Transport Canada and the Treasury Board of Canada Secretariat.

- GCpedia version
- YouTube version (http://www.youtube.com/watch?v=JRvY1SzWhl0)

Whenever Using Social Media:

Do	Don't
Use good judgment and common sense in all you do; your obligations as a public servant apply at all times.	Assume that a post is private, even when using a pseudonym; treat online posts as if they will be permanently and publicly available

	and attributable.
State clearly in your social media profile (used for professional purposes) that your views are your own, not those of your employer. **Remember:** This statement does not absolve you of your obligations as a public servant or the expected behaviours described in the Values and Ethics Code for the Public Sector and your departmental codes of conduct.	Disclose any classified, confidential, sensitive, or third-party information, or personal information about others.
Move work-related conversations to official channels (e.g., e-mail) so that there is a record of any guidance provided or decisions taken.	Use GC (Government of Canada) corporate symbols or signatures inappropriately. They are only for official use and their use is subject to the *Federal Identity Program Policy* and related standards. For more information, visit the Federal Identity Program website (http://www.tbs-sct.gc.ca/fip-pcim/index-eng.asp).
Maintain the impartiality and objectivity of the public service by not expressing opinions that could impair your ability to be seen as performing your duties in an objective or impartial manner.	Respond to requests for media statements or interviews related to your work (including from online media-like blogs) unless you are an authorized spokesperson. Send all media requests to your departmental media relations advisor.
Speak with your manager or Values and Ethics advisor if you are uncertain or have questions about any of your online activities.	Register or associate a GC (Government of Canada) e-mail address to a social media account unless it will be used explicitly for official or professional purposes.

▼ 2. Frequently Asked Questions about the Policy on Acceptable Network and Device Use

The following are examples of quick reference material that could be published on departmental intranets and wikis clarifying Policy requirements for authorized users of Government of Canada networks and devices, and Web 2.0 tools and services.

Are public servants allowed to use the Internet and Web 2.0 tools and services?

Yes! The use of, and open access to, the Internet through Government of Canada electronic networks and devices is essential to transforming the way public servants work and serve Canadians. Open access to the Internet, including Government of Canada and external Web 2.0 tools and services, enhances communication, collaboration and productivity, and encourages the sharing of knowledge and expertise to support innovation. Open access to the Internet, including Government of Canada and external Web 2.0 tools and

services, will be provided by departments by April 1, 2014, through a phased implementation of the new *Policy on Acceptable Network and Device Use* (the Policy).

What is considered to be acceptable use?

Appendix B of the Policy (/pol/doc-eng.aspx?id=27122&section=text#appB) provides examples of acceptable use of Government of Canada networks and devices. Permitted use of Government of Canada electronic networks and devices by authorized individuals includes:

- To perform activities as a part of their official duties;
- For career development and other professional activities; and
- For limited personal use that is conducted on personal time; that is not for financial gain; that does not incur any additional costs for the department; and that does not interfere with the conduct of business.

All use of Government of Canada electronic networks and devices must be in compliance with the *Values and Ethics Code for the Public Sector* and all other related Treasury Board policies and departmental codes of conduct and policies. Use of Government of Canada electronic networks and devices must not give rise to a real, potential or apparent conflict of interest or in any way undermine the integrity of the department.

What is considered to be unacceptable use?

Appendix C of the Policy (/pol/doc-eng.aspx?id=27122&section=text#appC) provides examples of unacceptable use of Government of Canada networks and devices. Unacceptable use refers to any activity that violates Treasury Board or organizational policy instruments or other published requirements, including, but not limited to, an activity or behaviour that:

- May give rise to criminal offences;
- Violates federal or provincial statutes;
- Impacts negatively on the performance of Government of Canada electronic networks and devices;
- Impedes departmental operations or the delivery of services;
- Breaches the "Duty of Loyalty" requirement for public servants (e.g., impairing or seen to be impairing the objectivity and impartiality of the public servant, the department or the Government of Canada); or
- Could result in liability.

What is a "Government of Canada electronic network or device?"

Electronic networks are groups of computers and computer systems that can communicate with each other, including but not limited to, the Internet, Government of Canada electronic data networks, voice and video network infrastructures, and public and private networks external to a department. Networks include both wired and wireless components. Devices include anything approved for use to access these networks or network resources, such as a desktop, laptop or tablet computer, memory devices such as USB (Universal Serial Bus) flash drives, or a smartphone.

How do the *Values and Ethics Code for the Public Sector* and my departmental code of conduct apply?

It is important to remember that the *Values and Ethics Code for the Public Sector* and your departmental code of conduct apply to online activities at all times, just as they do to your offline activities, irrespective of whether they happen at work or at home, or via a government or personally provided network or device.

Respecting the *Values and Ethics Code for the Public Sector* and your departmental code of conduct is a condition of employment in the public service. Violating them, including through inappropriate online activities, can have consequences for employment up to, and including, termination.

Respecting the *Values and Ethics Code for the Public Sector* in Online Activities

The following are examples of how the values and expected behaviours in the *Values and Ethics Code for the Public Sector* can be applied to public servants' use of electronic networks, electronic devices and social media, both officially and outside the office. These examples are not exhaustive. Public servants must also consult their departmental code of conduct and policy requirements.

Respect for Democracy

Public servants uphold Canadian parliamentary democracy and its institutions by ensuring that their online communications are non-partisan and impartial at all times, and do not engage in public discussion of departmental policies or elected officials that call into question their objectivity in carrying out their official duties.

Respect for People

Public servants demonstrate their respect for human dignity and the value of every person by ensuring their online communications are respectful of all individuals and groups of people, including colleagues, managers and members of the public.

Integrity

Public servants serve the public interest by ensuring, for example, that their official communications activities are not used for any inappropriate personal advantage and that government systems and equipment are not used to support personal businesses owned by them, their family or their friends.

Stewardship

Public servants demonstrate good stewardship by using electronic networks to share knowledge and information that will contribute to more effective program delivery, and by using network resources efficiently and effectively.

Excellence

Public servants demonstrate professionalism and excellence in the workplace by ensuring official communications respect Canada's official languages and by using social or other electronic media for team work, learning and innovation.

▼ 3. Use of External Storage Devices

The use of external storage devices can increase efficiency and data mobility, as well as reduce the amount of physical space needed to store information. However, these devices also present a risk for information and IT security, privacy breaches and theft. It is important that departments communicate to authorized individuals about the proper use of external storage devices to minimize the risk involved.

An external storage device can include all USB (Universal Serial Bus) storage devices (e.g., USB (Universal Serial Bus) drives, flash drives, thumb drives, jump drives, and memory sticks), portable hard drives and any other device with storage capacity connecting through a departmental corporate asset as well as other non-USB (Universal Serial Bus) based portable devices (e.g., CD (Compact Disc)/DVD (Digital Versatile Disc)s and SD cards). Note: It may be beneficial to provide examples of things that might not be top of mind but connect through USB (Universal Serial Bus)-based and have storage capacity (e.g., cell and smartphones, and cameras).

When developing departmental guidance or direction on the use of external storage devices, information provided may include:

- A description of the process for acquiring an external storage device;
- Departmental policy regarding unapproved or unencrypted storage devices connecting to the network;
- Requirements about the physical security of the device since responsibility for the security of the device resides with the user;

- Risks associated with the use of the device and the different security measures to minimize the risks including:
  - Storing the device in a locked cabinet when not in use;
  - Establishing strong passwords to protect unauthorized access to the device; and
  - Ensuring that the device is not left unattended, especially in a public area;
- Types/levels of encryption required for the different work being performed;
- Recordkeeping requirements of files stored on the devices (e.g., files on the device are considered copies of the original and they are not the primary record);
- Backing up information since it may not be recoverable if erased;
- Requirements about personal information being stored on external storage devices:
  - Is it permitted? and
  - If so, what types of personal information are permissible and should it be encrypted?
- Procedures to follow if a storage device will be holding personal information (e.g., refer to the *Guideline for Privacy Breaches* (/pol/doc-eng.aspx?id=26154));
- A disclaimer stating that the department is not responsible for the loss or corruption of personal data stored on a device;
- Who to contact in the event of damage, loss or theft of a storage device or if users have questions regarding an external storage device;
- References to other Government of Canada or departmental policies that support the acceptable use of devices; and
- Consequences of unacceptable use.

Note: The Treasury Board of Canada Secretariat *Information Technology Policy Implementation Notice (ITPIN)* outlines the mandatory requirements for departmental use of external storage devices.

▼ 4. Security Reminder Bulletin

The following is an example of reminder material that departments could send to authorized individuals in order to meet the requirements of Section 6.1.2 of the Policy (/pol/doc-eng.aspx?id=27122&section=text#cha6). This reminder can also serve to offer learning opportunities for authorized individuals.

Your Monthly Security Reminder: Handling Your BlackBerry

A departmental BlackBerry device comes with many responsibilities for its protection and the data that it contains. If you have been issued a departmental BlackBerry device, please keep the following in mind:

- BlackBerry voice communications are not considered secure, and as such, the device must not be used to discuss sensitive information when used in phone mode. Blackberries deployed with Secure/Multipurpose Internet Mail Extensions functionality enabled can be used to transmit data through electronic messaging up to and including the level of Protected B. Classified information cannot be transmitted, either by voice or data on a BlackBerry device;
- PIN (Personal Identification Number)-to-PIN (Personal Identification Number) messaging, unlike BlackBerry e-mails, is unencrypted, which means that the messages are not secure and should only be used for unclassified and emergency communications;
- If an employee no longer needs his or her BlackBerry, it should not be used by another employee since its PIN (Personal Identification Number) number is a unique identifier for the device. If your BlackBerry is "recycled," a PIN (Personal Identification Number)-to-PIN (Personal Identification Number) message meant for you would unintentionally be sent to the employee who now has the device;
- BlackBerry PIN (Personal Identification Number)-to-PIN (Personal Identification Number) and text messages are subject to Access to Information and Privacy (ATIP (Access to Information and Privacy)) requests;
- BlackBerry e-mail messages are vulnerable to the same threats as other e-mail programs; these threats can include viruses, Trojans and phishing attacks. If you receive an e-mail and do not recognize the sender, do not open it--simply delete it;
- When using the camera feature of a BlackBerry, be careful not to take photos of sensitive information or equipment;
- Photos taken with a BlackBerry are subject to ATIP (Access to Information and Privacy) requests and to the same records retention criteria as other documents and correspondence;
- Photos of colleagues should not be taken with a BlackBerry or posted on social media without their consent. In addition, you should carefully consider the photos that you choose to store in your Outlook mailbox or on departmental network drives, since they take up large amounts of valuable disk space;
- Some devices will save key metadata (i.e., geolocation) whenever a photo is taken. This information may have privacy or operational security implications and should be carefully scrutinized before the posting of photos; and

- If your BlackBerry is lost or stolen, report it immediately by using the Self-Service tool or by contacting [contact name].

Security: It's everyone's responsibility!

▼ 5. Smartphone Etiquette

The use of smartphones is prevalent in a mobile workplace. Although smartphones can enable greater connectedness with colleagues and support increased productivity, they can also be disruptive. Expecting a common sense approach to using these devices is not a guarantee. To ensure that they are used in the manner for which they were intended, Shared Services Canada (SSC (Shared Services Canada)) has developed an Interim Operating Standard on the Acceptable Use of Cellular Devices, which departments not receiving their network services from SSC (Shared Services Canada) may find useful. Departments may also find it worthwhile to promote awareness of smartphone etiquette. The following table of key messages could be used to communicate information about this subject:

Work-related Device	Personal Device
• Do not lend the phone or share the access password; • Limit the presence and use of smartphones during meetings; • Choose professional ringtone types and adjust volume settings to vibrate or low; • Keep personal use of department-issued devices to a minimum; • Select appropriate places when using cellphones to conduct business (e.g., private area); • Do not bring cellular phones into secure discussion areas; • Use devices appropriately in public places (e.g., restaurants, theatres and hospitals); • Refrain from putting the phone on speaker mode when talking about work-related issues in earshot of others; • Avoid incurring new costs to the organization (e.g., downloading of personal applications or new ringtones); • Know the rules about using the camera (if activated) to avoid the risk of potential security incidents or privacy breaches; and • Do not disclose any classified,	• Adjust volume settings to vibrate or low while at work; • Avoid bringing a personal device into a work-related meeting; and • Minimize the use of personal devices at work (e.g., by taking personal calls on scheduled breaks or at lunch).

confidential, sensitive, or third-party information, or personal information about others.	

▼ Appendix G: Sample Notifications

This appendix provides examples of different types of notifications that could be used to inform authorized individuals of the requirements of the *Policy on Acceptable Network and Device Use* (the Policy).

The notifications include alerts about monitoring practices or user acknowledgement of the terms and conditions of the use of Government of Canada networks and devices, including the use of Web 2.0 tools and services. Some of the examples below could be displayed daily upon initial account sign-in or at scheduled intervals, or presented to new employees during orientation, depending on departmental circumstances and needs.

▼ 1. Employees Network Sign-On Notification

[This notification can be displayed on a regular basis when employees sign on to the network. A best practice is to display the notification on a daily basis.]

Access to this system is restricted to authorized individuals only.

[Department name] reserves the right to monitor all electronic resources and subsequently record all forms of communication and transmission for work-related purposes to ensure proper network performance and security, protection of government assets, optimal use of network resources and compliance with relevant legislation and policies. Monitoring to gather information to investigate and resolve suspected cases of unacceptable use may occur at any time without further notification.

All blocking and monitoring will be done in compliance with the Privacy Act and the Canadian Charter of Rights and Freedoms.

The Policy on Acceptable Network and Device Use is available on the Treasury Board of Canada Secretariat website.

▼ 2. Employee Reminder Notice about the Policy on Acceptable Network and Device Use

[This notification requires authorized individuals to acknowledge and accept that they have read and understood the Policy. Notification and acknowledgement could be monthly or quarterly to ensure that the expectations of acceptable use, the monitoring practices of the department, and the consequences of

unacceptable use are communicated and acknowledged. The notification may be used in its entirety or in part, depending on departmental needs and strategy.]

Policy on Acceptable Network and Device Use

I have read the Policy and acknowledge that:

- *I will use departmental networks and devices for activities related to my official and professional duties in compliance with the Policy;*
- *I will abide by the expectations of acceptable use of networks, devices, and Web 2.0 tools and services outlined in the Policy, the Values and Ethics Code for the Public Sector and all other related Treasury Board policies and departmental policies and code of conduct;*
- *I am aware that employee activities on Government of Canada networks and devices are monitored for the purposes of assessing system performance, protecting government assets and ensuring compliance with Treasury Board and departmental policies and codes of conduct;*
- *I understand that special monitoring of departmental networks and devices to investigate and resolve suspected cases of unacceptable use may be conducted without notice;*
- *I have read the Policy and acknowledge that:*
    - *If I choose to use the network for limited personal use and store personal information on the network or devices, it will be at my own risk; and*
    - *I understand that all information that is transmitted and stored on departmental electronic systems may be subject to public access requests under the Access to Information Act and the Privacy Act; and*
- *I understand that unacceptable use of electronic networks, devices and Web 2.0 tools and services can have employment consequences up to, and including, termination.*

▼ 3. Acknowledgement of Receipt and Understanding of the Policy on Acceptable Network and Device Use

[Another form of acknowledgement and understanding of the Policy is through a form that could be included as part of a new employee orientation package or when granting the use of Government of Canada networks and devices.

This form may be useful to managers to help generate awareness about the acceptable use of electronic networks, devices and Web 2.0 tools and services to authorized individuals who are new to the department. Presenting the form during orientation sessions can confirm that the authorized individual has

received, read and understood the Policy. It is another potential measure to ensure that the individual is aware of the expectations of acceptable use, the departmental monitoring practices and the consequences of unacceptable use.]

I [insert name] acknowledge that:

1. *I have been informed of the requirements of the* Policy on Acceptable Network and Device Use *(the Policy);*
2. *I understand the terms of use of networks, devices, and Web 2.0 tools and services;*
3. *I have been made aware of the expectations of acceptable use and I agree to abide by them;*
4. *I realize that failure to comply can have employment consequences up to, and including, termination;*
5. *I understand that all information that is transmitted and stored on the departmental electronic systems may be subject to public access requests under the* Access to Information Act *and the* Privacy Act*;*
6. *[Department name] reserves the right to gain access to the systems and its contents to conduct routine and special monitoring processes for acceptable use; and*
7. *I have been informed of the procedures to follow when reporting suspected instances of unacceptable use and who to contact if I have any further questions about the acceptable use of networks and devices.*

Name: Date:
Supervisor:Date:
Witness: Date:

Footnotes

1 Under Section 6.2 of the Policy, for departments that receive their network services from Shared Services Canada (SSC (Shared Services Canada)), the deputy head of Shared Services Canada is responsible for managing tools to support monitoring. SSC (Shared Services Canada) is also responsible for providing reports about the use of Government of Canada electronic networks and devices, and Web 2.0 tools and services to assist deputy heads in the identification, investigation and implementation of corrective action on issues that arise regarding unacceptable use.

Expand All | Collapse All

Date Modified:

2014-06-09