Internet and E-mail Code of Conduct

Scotiabank™
I. Introduction

a. Background
Information technology and services, such as the Internet, e-mail and internal information systems, offer efficient and effective ways of communicating, researching and conducting business worldwide. However, the use of these resources is not without risk. For example, inappropriate online behaviour can lead to the accidental or improper disclosure of confidential information, virus attacks, fraud and reputational damage, or impede the efforts of the Scotiabank Group1 and its employees to maintain a respectful work environment.

Accordingly, the Scotiabank Group and its employees have a responsibility to maintain standards for the appropriate use of information technology and services so that our ability to provide quality services to our customers and co-workers is not impaired.

b. About this Policy
The Internet and E-mail Code of Conduct (“the Internet Code”) is a mandatory supplement to the Scotiabank Guidelines for Business Conduct (“the Guidelines”), and applies to all officers and employees of the Scotiabank Group worldwide.2 It also applies to casual or contract employees and other third parties who use Scotiabank’s information technology or services.

The Internet Code provides specific guidance with respect to the appropriate use of information technology and services including, but not limited to, the Internet, e-mail and internal networks and information systems. As with the Guidelines, adherence to the Internet Code is a condition of employment at Scotiabank. Any use of information technology and services that breaches the Guidelines or the Internet Code is a serious matter, and could result in discipline up to and including termination of employment.

c. Scotiabank Group’s Ownership of Internet, E-mail and Internal Information Resources
The Scotiabank Group provides its employees with a range of information technology and services in the course of their employment. These can include, for example: access to desktop or laptop computers; handheld devices, such as personal digital assistants (PDAs) or cellular phones; e-mail; the Internet; internal networks and information systems; and instant messenger services. These facilities can be provided to you directly (e.g., via your Scotiabank-issued desktop, laptop, PDA or cellular phone) or indirectly (e.g., VPN access to the Internet from a personal computer at home).

Regardless of the type of information technology and service provided, or whether it is provided to you directly or indirectly, these facilities are the property of the Scotiabank Group. While reasonable, occasional personal use of the Internet and e-mail is permitted, these services have been provided to enable you to perform your job on behalf of the organization. (See “Quick Reference”.)

d. Applicability of this Policy to Your Non-Scotiabank Internet and E-mail Use
As a private citizen, you are entitled to express your personal views, but bear in mind that inappropriate Internet use outside the workplace could subject Scotiabank or its employees or customers to legal, reputational, security or other risks. For example, an Internet posting that breaches customer privacy is a breach of the Guidelines and of privacy regulations, even if posted from a non-Scotiabank computer using non-Scotiabank Internet facilities.

If you choose to offer your personal opinions online, use common sense and be careful not to give the impression that you are speaking on behalf of Scotiabank or expressing a Scotiabank-approved perspective. Keep in mind that anyone – customers, managers, fellow employees, family members and competitors – can easily read remarks posted on public websites, and that remarks or other information may be impossible to remove once posted.

1 The words “Scotiabank”, “Scotiabank Group”, “Bank”, “Chain of Communication”, “confidential information”, “confidential business information”, “inside information”, “Legal Department”, “manager”, “personal information” and “policies, procedures and processes”, where used in this policy, have the same meaning as in the Glossary of the Scotiabank Guidelines for Business Conduct.
2 Policy Maintenance: Group Compliance and Information Security & Control are the joint custodians of the Internet and E-mail Code of Conduct, and are responsible for ensuring that it remains current and appropriate.
II. Appropriate Use of the Internet and E-mail

The six Guiding Principles contained in the Guidelines apply to all Scotiabankers at all times. However, four of the Guiding Principles are particularly relevant to appropriate use of information technology and services:

1. **Follow the Law Wherever Scotiabank Does Business**

Never use information technology or services to engage in an activity that is illegal or unethical or would bring the reputation of the Scotiabank Group into disrepute. This includes, but is not limited to: industrial espionage;3 sabotage; “phishing”;4 identity theft; hacking, or possessing software designed for hacking or to otherwise break systems security; pyramid schemes; gambling; or accessing, viewing, posting, transmitting, downloading, storing or distributing material that is pornographic, discriminatory, abusive or similarly offensive, unprofessional or a breach of copyright laws.

Some laws are particularly relevant to the use of information technology and services:
- **Intellectual property rights:** You may not download any third-party intellectual property – including software, creative works or other materials – if to do so would violate any vendor/owner rights. Be aware that software available over the Internet, including free and demo software, and upgrades to software already in use, may have licensing restrictions which are not readily apparent. If you have secured internal and third party permission to download intellectual property, ensure that you protect it from further use by unauthorized persons.
- **Public company and financial services regulations:** Remember that all of the laws and regulatory requirements that apply to the Scotiabank Group and its employees in the “real world” also apply online. For example:
  - There are many rules surrounding the disclosure of information about publicly traded companies, including disclosure via the Internet. Breaching these rules may subject you, Scotiabank and its officers and directors to severe penalties.
  - In many countries Scotiabank is subject to regulation with respect to advertising, marketing and other public communications. Therefore, always ensure that websites, online advertisements, postings on public websites that relate to our products and services and direct marketing campaigns (e.g., telemarketing or the unsolicited e-mailing of customers for marketing purposes) are subjected to the appropriate Scotiabank, subsidiary or business line approval procedures.

Quick Reference:

**What is reasonable, occasional personal use?**

Scotiabank permits reasonable, occasional personal use of the Internet and e-mail while at work. Examples of reasonable, occasional personal use include, but are not limited to:
- briefly checking a personal e-mail, social networking or instant messaging account (e.g., over your lunch break);
- accessing online banking or a personal brokerage account from time-to-time; and
- visiting an external website to, for example, check the weather forecast, or quickly make an online purchase.

**Examples of personal Internet and e-mail use that are not permitted include, but are not limited to:**
- sending a high volume of personal e-mails, instant messages, etc.;
- constantly or very frequently monitoring a personal e-mail account, blog, social networking site, etc., throughout the workday;
- downloading or uploading games, music or videos, or other peer to peer (p2p) file sharing activities;
- using Scotiabank Group e-mail or Internet facilities to engage in personal political activities, outside employment or outside business activities;
- excessive personal trading (e.g., day trading);
- online gambling of any kind;
- viewing, circulating or posting materials that are likely to cause offence or humiliation to any employee or customer (e.g., materials that: are of a sexual nature; promote illegal, unethical or violent behaviour; or promote the denigration or superiority of any ethnic, religious or other identifiable group); or
- any use that a reasonable person would perceive as having a negative impact on job performance or productivity.

---

3 “Industrial espionage” means attempting to obtain confidential business information by dishonest means.
4 In a “phishing” attack, individuals send e-mails impersonating legitimate businesses in an attempt to trick the recipients into disclosing private information that could be used for fraudulent purposes. Often the fraudulent e-mails ask for account or transaction verification, or warn that a customer’s account has been compromised. Like other financial institutions, Scotiabank Group entities and customers are often targeted by phishing scams.
2. Conduct Yourself Honestly and with Integrity

Scotiabank’s policy is to be truthful and non-misleading in all communications and representations, written and verbal. This includes communication by e-mail, or using web-based public forums such as Internet “blogs”, chat rooms, newsgroups, social networking websites, etc.

Some rules to follow when using electronic communications or participating in web-based forums include the following:

- Always use appropriate and professional language in electronic communications, whether intended for a customer or an internal recipient. Bear in mind that electronic communications such as e-mail or instant messenger can be misdirected, accidentally viewed by persons other than the intended recipient or subject to scrutiny by internal or external third parties (e.g., internal or external audit, Security and Investigation or judicial or regulatory authorities).
- Unless you are a specially designated person for whom it forms part of your normal duties, refrain from commenting on the Scotiabank Group, its business activities or competitors in any online public forum. This includes making anonymous postings.
- Never post material obtained from or associated with the Scotiabank Group that is damaging to the interests of or embarrassing to the Scotiabank Group.
- Do not use Scotiabank logos, trademarks, trade names or other proprietary materials without prior approval or for any other purpose than the furtherance of Scotiabank's legitimate business objectives. Ensure that you follow Scotiabank, subsidiary or business line guidelines when using Scotiabank Group logos, trademarks, and/or trade names online.

3. Respect Confidentiality, and Protect the Integrity and Security of Assets, Communications, Information and Transactions

Scotiabank has rules in place designed to protect the privacy and security of confidential information and assets while using information technology and services. These include the following:

- Under no circumstances may inside or confidential information – including information about customers or the Scotiabank Group – be posted to any public or non-Scotiabank sites, including blogs, bulletin boards, chat rooms or social networking sites. This includes information on Scotiabank’s security procedures, practices or vulnerabilities, as well as images or representations of Scotiabank facilities.
- Unless you have a legitimate business reason and proper authorization, never use your information technology or systems privileges to access customer or employee personal information (e.g., profiles), or confidential business information about Scotiabank, its customers or your fellow employees.
- Ensure that you do not compromise the confidential information of customers, employees or Scotiabank. Because no guarantee of privacy or confidentiality can be given to e-mail messages or other electronic communications or documents once they leave Scotiabank Group networks and enter the Internet, consider the confidentiality level of your message before transmitting. Use caution when forwarding e-mails or using the “reply all” feature to avoid unnecessarily transmitting confidential information to those without a business need.
  - Some privacy laws restrict the transmission of some kinds of personal information between legal entities or from one legal jurisdiction to another. Make sure you understand Scotiabank’s and your subsidiary’s legal responsibilities before e-mailing or otherwise transmitting employee or customer personal information between legal entities or across national borders. If in doubt, consult your manager or the Legal Department.
- Unless authorized by Information Security and Control, or set out in the compliance policies, procedures or processes for your line of business:
  - do not store confidential information on your home computer; and
  - never use your personal e-mail account (e.g., a non-Scotiabank e-mail account), another external Internet platform or service (e.g., Hotmail, G-mail, Yahoo Briefcase, MSN Messenger, Facebook, etc.), or external instant messenger service (e.g., PIN2PIN, SMS, MMS, etc.) to transmit or store confidential information or conduct business with customers.
- Be alert for fraudulent activities and social engineering techniques such as pretexting or phishing. Report suspected phishing or social engineering attacks against Scotiabank by e-mailing phishing@scotiabank.com. Report criminal or fraudulent activities to your manager or a more senior officer, or using the process described in the Guidelines.

---

5 See Footnote 1 for definitions of “inside information” and “confidential information”.

6 “Social engineering” is a collection of techniques used to trick employees into divulging confidential personal or business information or granting access to secure systems.

7 Pretexting is a social engineering technique used to obtain an individual’s personal information (passwords, etc.) by posing as that individual, usually over the telephone or by e-mail.
4. Treat Everyone Fairly, Equitably and Professionally, Whether Customers, Suppliers, Employees, or Others Who Deal With Scotiabank

Your actions are expected to be consistent with the spirit and intent of the Canadian Human Rights Act and other relevant human rights and anti-discrimination laws that apply to subsidiaries or Scotiabank’s operations within or outside of Canada. Any use of the Internet, e-mail or other information technology that is harassing or otherwise inconsistent with these principles will not be tolerated.

You are expected to use good judgment whenever you send an e-mail or other type of electronic communication. Consider carefully whether the recipient(s) would consider the communication to be offensive, harassing, threatening, annoying, unprofessional or otherwise unwelcome. If in doubt, consult your manager.

III. Scotiabank Group’s Right to Monitor and Restrict Access

Scotiabank has a policy of open access to the Internet, and does not typically restrict access to most websites. However, Scotiabank reserves the right to restrict access to the Internet, e-mail and internal information systems for any reason, at any time and without notice.

In addition, to protect Scotiabank and its employees, some Scotiabank entities employ technology to block access to websites that contain prohibited material. If you inadvertently access a website that contains prohibited material, immediately leave the site and advise your manager.

Your use of Scotiabank’s information technology and services may be monitored at any time to identify and/or act upon unusual, inappropriate or suspicious activities that may indicate a breach of the Guidelines, applicable laws, or other Scotiabank Group policies. For some employees, this is a regulatory requirement. This includes monitoring the content of your e-mails or other communications (e.g., instant messages, postings, etc.) and the contents of your desktop, laptop or handheld computer. In addition, a record of all Internet and intranet sites visited may be captured and logged, including personal web-based e-mail accounts, social networking sites, blogs or chat rooms.

Scotiabank also monitors general Internet chatter, including any postings on public websites, blogs, chatrooms and social networking sites. This is done in order to ensure compliance with applicable laws and Scotiabank’s policies, collect marketing or public affairs insights or for other purposes related to the protection of Scotiabank or customer assets or reputation.

Conducting business with customers using the Internet or e-mail

Business with customers should be transacted securely, using approved online systems, services and products. These are supported by customer agreements, back-up systems and provisions for documenting and keeping records of transactions. Approved systems also include security features such as customer/sender/transaction authentication, encryption and other measures to verify the authenticity, integrity and confidentiality of the customer communication.

Customers inquiring about doing business via e-mail should be advised that it is not secure, and there is no guarantee of confidentiality or delivery.

Some business units have developed customer agreements, detailed operating procedures and verification procedures (e.g., obtaining telephone confirmation of e-mail instructions) to accommodate customers who still wish to conduct business or correspond using e-mail. Exception as provided for in these procedures, do not transmit confidential information, accept payment or other important instructions or conduct business with customers via the Internet or e-mail.

8 Unless such monitoring is prohibited by local law.
### Additional Sources of Information and Guidance

<table>
<thead>
<tr>
<th>ISSUE</th>
<th>SOURCES OF GUIDANCE OR ADVICE</th>
</tr>
</thead>
</table>
| Additional guidance on the appropriate use of information technology or systems | Speak to your manager or a more senior officer as per the Chain of Communication  
(Note: your manager may consult with your Compliance Department, the Information Security and Control department or your local systems administrator for assistance) |
| Information educational materials and standards related to Internet, e-mail and network security | Visit the Information Security and Control website at http://info.security.bns  
or  
Send an e-mail to AskSecurity@scotiabank.com |
| Information on safe computing practices                               | Visit the "Safe Computing Practices" section of www.scotiabank.com  
or  
Send an e-mail to AskSecurity@scotiabank.com |
| Assistance developing customer agreements and operating procedures for conducting business with customers via e-mail | Legal Department  
and  
Information Security and Control (Send an e-mail to AskSecurity@scotiabank.com) |
| Reporting suspected phishing or social engineering attacks against a Scotiabank entity | Send an e-mail to phishing@scotiabank.com |
| Suspected fraudulent or criminal activity                               | Your manager or a more senior officer as per the Chain of Communication  
or  
Contact the Security and Investigation department |
| Reporting Spam                                                        | Contact your local systems administrator |

---

**Legal Department**  
**Information Security and Control**