IT Acceptable Use Policy

Policy Owner:	**Information Technology**
Policy Applies to:	All Sobeys Inc. employees
Effective:	November 24, 2016
Last Updated:	November 24, 2016

Objective

The objective of this policy is to outline the acceptable use of Sobeys' information systems and resources. This Policy is intended to accompany the Sobeys Code of Business Conduct and Ethics (the "Code") to help protect Sobeys, Sobeys' employees and Sobeys' customers.

Definitions

- **Authorization** –The concept of allowing access to resources only to those permitted and approved to use them.
- **Employee –** Any individual employed by any subsidiary of Sobeys Inc. including temporary and student employees with access (through a username and password), to Sobeys' information systems.
- **Internet –** The Internet is a worldwide communications network designed to facilitate data transmission and exchange.
- **Internet E-mail** – E-mail exchanged between a Sobeys e-mail address and a non-Sobeys e-mail address. This e-mail is transmitted over the Internet.
- **Internal E-mail** – E-mail exchanged between Sobeys e-mail addresses. This e-mail is transmitted within the Sobeys electronic communication network.
- **PDA** – Personal Digital Assistant.

Scope

This policy applies to all employees of Sobeys and its subsidiaries regarding the use of network systems and services including but not limited to:

a) Communication systems such as e-mail systems, instant messaging, text messaging, SMS messaging, etc.
b) The Internet and associated Internet services.
c) Information handling and access control.
d) Devices owned by Sobeys used to communicate with or across the Internet. Devices include but are not limited to computers (laptops, desktops and servers), PDAs (including Blackberrys) and cell phones.

This Policy is designed to:

a) Protect the reputation and resources of Sobeys and its customers from irresponsible or illegal activities.
b) Ensure privacy, security and reliability of Sobeys' information by describing appropriate uses of e-mail and the Internet.
c) Establish policies for the acceptable use of Sobeys' e-mail and Internet resources.

This Policy is also intended to inform employees that the Internet is not a confidential medium. Some services may provide confidentiality of information transmitted over the Internet but this is not provided by default. Discretion should be used regarding information sent through a web browser or through e-mail to non-Sobeys' e-mail addresses or web sites, because this information may be copied or intercepted by unauthorized third parties.

Responsibilities

It is the responsibility of every employee of Sobeys to assist in maintaining the integrity, confidentiality, and availability of Sobeys' IT systems by utilizing these systems for Sobeys' business purposes only.

Acceptable Use Policy

General Use and Ownership

1. Use of any Sobeys computer system indicates agreement to comply with all applicable provisions of the Sobeys Code of Business Conduct and Ethics, including specifically section 3.5.
2. Computers and computer accounts provided by Sobeys are company assets that are to be used to execute business activities on behalf of Sobeys. Documents (including e-mail messages) created, stored, sent or received on Sobeys computers are the property of Sobeys.
3. Confidential Information must be appropriately protected and used with discretion. Employees should refer to section 3.4 of the Code for specific details regarding Confidential Information.
4. Employees must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending chain letters, sending jokes to numerous people, spending excessive amounts of time on the Internet, playing games or engaging in online chat groups.
5. For security and network maintenance purposes, authorized individuals within Sobeys may monitor equipment, systems and network traffic at any time.
6. Sobeys has the right, but not the duty, to audit or monitor any of its IT Systems or networks to ensure compliance with this policy. This includes, but is not limited to, monitoring sites visited by employees on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded or uploaded by users to the Internet, and reviewing e-mail sent and received by users.

Information Handling and Disclosure

1. All Sobeys' electronic information must be handled (e.g. stored, processed, transmitted, retained, released, destroyed) in a secure manner with due care.
2. Computer and network Confidential Information controls must include the following:
    a. Access controls ensuring select individuals have access based on business need.
    b. Encryption controls if Confidential Information is to be transferred electronically (e.g., FTP transfers).
    c. Confidential Information must not be posted to any external web site, forum, blog, etc.
    d. Employees have an obligation to protect Company property and should refrain from copying Confidential Information to laptop hard-drives, CDs or DVDs, USB memory

drives (or other external storage devices) except in cases of business necessity and where other steps are taken to protect the Confidential Information.

e. Company assets that have data storage capabilities must be secured at all times when not in use.
f. In the event Confidential Information is required and approved for electronic access by any third parties, an IT Security review must be performed to ensure their internal controls and processes are sufficient to protect this information.
g. Credit card data must be secured at all times in any format (e.g., computer display screens, receipts, etc) and must not be stored electronically on any systems or sent through any messaging technologies (e.g., email's, text's, FTP transfers, etc).
h. Approval to remove or copy customer lists or any other customer personal information from any IT System will be provided **only** through a written approval process requiring the signature of the CMO, CFO, or CIO.

Network / System Access

1. Employees must not access or attempt to access any Sobeys system for which they have not been provided authorization.
2. Passwords must not be shared by employees. Accountability for employee actions on the network and within applications is associated directly to employee login credentials (username and password). As such each employee is responsible for actions performed under their credentials and will be held accountable.
3. Employees must never use or install any computer or device onto Sobeys' computing network that is not approved for use. Such devices include but are not limited to wireless access points and routers.
4. Employees must never allow external parties to connect any device to Sobeys network without prior written approval.
5. Employees must never install software on any Sobeys computer unless it has been approved. Any unauthorized or unlicensed software found on any Sobeys computer will be removed by Sobeys IT.

Email and other Communication Systems

1. Employees must be mindful that all electronic communications can be copied by others.
2. Sobeys' communication systems shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments. In the event an employee receives an e-mail with this type of content from another employee, they should immediately report the matter to their manager or direct supervisor.
3. Employees must never send unsolicited messages of any kind, including "junk mail" and or "spam" to anyone.
4. Employees must never respond to unsolicited messages such as "spam". Responding simply validates your e-mail address.
5. Use precaution when opening attachments in e-mails. For example, if you are not expecting it and do not recognize the sender, you should probably delete the entire e-mail.
6. Precautions must be taken when sending messages to ensure recipient lists are accurate. Messages intended for internal e-mail recipients must be carefully examined to ensure Internet e-mail recipients are not included in the to, cc, or bcc fields.

Internet Access

Sobeys has invested in comprehensive security controls that help protect Sobeys' assets and our employees, however there are risks associated with the Internet for which the only defence is safe surfing habits. The following rules must be adhered to:

1. Employees must never download, transmit, or store any material that is prohibited. See Appendix A of this document for a list of prohibited materials.
2. Employees must never attempt to monitor any communications by any means. IT personnel may monitor for support and troubleshooting purposes only and are exempt for this reason.
3. Employees must never introduce malicious programs, viruses, or code into Sobeys' systems or networks.
4. Some occasional personal use of Sobeys' computers is permitted.
5. Employees must at all times use caution to maintain Sobeys' good corporate reputation.

Policy Enforcement

Sobeys reserves the right to access, and disclose all information, messages and/or other communications originating from Sobeys over its electronic communications network, for various authorized reasons which may include, but are not limited to:

1. Access for business needs
2. Employee illness, vacation or absence
3. As required by law enforcement and or legal processes

Such access will be done through a formal request and approval process involving management.

Disclaimer of liability

Sobeys is not responsible for material viewed or downloaded by users from the Internet. The Internet contains millions of pages of information. Users are cautioned that many of these pages include inappropriate content that may be offensive or even sexually explicit. Search requests with good intentions may inadvertently lead to sites with inappropriate content. In addition, having an e-mail address may lead to receipt of unsolicited e-mail containing inappropriate content.

Appendix A

Employees of Sobeys are prohibited from creating, transmitting, distributing, forwarding, downloading and/or storing anything via Sobeys' computers and electronic communications network which:

(a) infringes any copyright, trademark, trade secret, or other intellectual property right;

(b) is obscene, profane, pornographic or sexually explicit;

(c) is libellous, defamatory, hateful, or constitutes a threat or abuse;

(d) encourages conduct that would constitute a criminal offence or give rise to liability on the part of the Company, its directors or officers;

(e) harasses the receiver, whether through language, frequency, or size of messages;

(f) is considered e-mail junk, spam or chain e-mail;

(g) forges or misrepresents the sender's identity;

(h) divulges private and/or confidential information related to Sobeys' business or its employees;

(i) violates any of Sobeys' policies or the Code of Business Conduct and Ethics;

(j) solicits Company employees for selling products or services; or

(k) is otherwise unlawful.