Exhibition Place

Item No. 11

November 1, 2012

To: The Board of Governors of Exhibition Place

ACTION REQUIRED

From: Dianne Young, Chief Executive Officer

Subject: Information & Technology Acceptable Use Policy – Board Employees

Summary:

This report recommends that an Information & Technology Acceptable Use Policy for employees of the Board be implemented and that the current policies entitled "Computer/Telephone Usage" and "Social Media Use" be deleted. The specific language within the new policy is in substance identical to the policy adopted by the City's Information & Technology Division on February 6, 2009, but modified to address the particular nature of Exhibition Place.

The current Computer/Telephone Usage policy is incorporated in the new policy and the Social Media Use Policy will be integrated within the "Designated Internet Usage" of this new policy.

Recommendations:

It is recommended that the Board:

(1) approve an Information & Technology Acceptable Use Policy for Board Employees, as outlined in Appendix "A"; and

(2) delete the existing "Computer/Telephone Usage" and "Social Media Use" Policies from the Human Resources Manual.

Financial Implications:

There are no financial implications arising from the recommendations in this report.

Decision History:

The Exhibition Place 2009 – 2012 Strategic Plan had an Organizational & Staffing Goal to *Review and revise our corporate systems* and as a Strategy to support this Goal *we will complete an annual review of By-Laws, Policies and Procedures of the Board of Governors and CNEA Board of Directors.*

At its meeting of November 3, 2006, the Board approved of a consolidated Personnel Manual for Exhibition Place employees, wherein the Computer/Telephone Usage Policy was included; and at its meeting of December 16, 2011, the Board approved a Social Media Use Policy, wherein said policy is currently being reviewed in detail and will be revised and presented to the Board, if necessary, at a later date for consideration.

Issue Background:

Given the growth and constant changes in information and technology usage by employees, a detailed policy is necessary as a guideline for staff.

Comments:

The new Information & Technology Acceptable Use Policy attached replicates most of the directions found within the City of Toronto's "Acceptable Usage Policy" and is much more detailed with respect to the responsibilities of Board employees in relation to use of the information and technology resources.

Contact:
Fatima Scagnol
Corporate Secretary
Tel: 416-263-3620
Fax: 416-263-3690
Email: FScagnol@explace.on.ca

_____

Dianne Young
Chief Executive Officer

1. Purpose

The purpose of this policy is to establish the accountability, responsibility and service excellence expectations surrounding the use of the Board's Information and Technology Resources (I&T Resources). A breach of this policy may result in an exposure to the Board's information. This exposure, should it materialize, could result in a legal and/or administrative risk to the Board.

I&T Resources are to be used solely for Exhibition Place business purposes.

Authorized Users should use a "common-sense" approach when using I&T Resources. All Authorized Users are expected to carefully consider the actions they take prior to using I&T Resources and should contact their direct report within the Senior Management Team for advice and clarification.

2. Application

This policy applies to "Authorized Users" including "Remote Access Users" as defined in the "Definitions" section.

Individual divisions may create additional operational needs documents to meet specific divisional business objectives provided that:

- This Information & Technology Acceptable Usage Policy is a minimum standard and any operational needs documents do not nullify any portion of this policy; and
- The Chief Financial Officer is consulted as part of the Divisional approval process.

3. Definitions

- **"Authorized Users"** means individuals who have been given permission to use the Board's information and technology resources as defined and includes Remote Access Users as defined.

- "**Board"** means the Board of Governors of Exhibition Place.

- **"Chief Executive Officer"** means the CEO appointed by the Board.

- **"Chief Financial Officer"** means the CFO appointed by the Board.

- **"City Solicitor"** means the Solicitor of the Board appointed by the City of Toronto.

- **"Corporate Secretary"** means the CS appointed by the Board.

- **"Data Transfer"** means the movement of information or data from one information technology resource to another regardless of the method of transfer.

- **"I&T Management Team"** (ITMT) consists of the CFO, CEO, and Manager of IT/Telecom. In the absence of the CEO or CFO, authority will be delegated to the CS.

- **"Information and Technology Resources"** (I&T Resources) include, but are not limited to: desktop computers, monitors, printers, notebooks, tablet computers, handheld computers, scanners; computer peripherals such as: CDRW drives, DVDRW drives, zip drives, digital projectors; peripherals such as: storage devices and power supplies; personal digital assistants (PDA's); network devices; software such as: Corporate software, off-the-shelf software packages, software covered by enterprise license agreements and volume license agreements (including maintenance and support); data created using any of the Board's I&T Resources; Internet access; e-mail; telephones and voice mail; facsimile machines (if connected to the Board's computer network); photocopiers (if connected to the Board's computer network); and mobile devices.

- **"Internet Designated Sites"** means those internet sites to be used for Board business and determined by the ITMT.

- **"Internet Designated Usage"** means those employees determined by the ITMT that will have access to the designated Internet sites wherein such sites will only be used for business purposes and will be accessible only by these designated Authorized Users. An up-to-date listing of designated users will be managed by the CFO and any requests for Internet Designated Usage must be submitted in writing with an explanation to the CFO by the Senior Manager.

- ***Municipal Freedom of Information and Protection Privacy Act*** and ***Personal Health Information Act*** will be referred to as the *Acts.*

- **"Mobile Devices"** are portable computing devices that allow you to store, organize, access and transmit information. Mobile devices include, but are limited to: cell phones, land-line phones, notebooks, PDAs, tablet computers, and handheld computers. Mobile Devices are I&T Resources.

- **"Peripherals"** are a computer device, such as a CD ROM, USB storage device or printer that is not part of the essential computer. Peripherals are I&T Resources.

- **"Personal Information"** (and personal health information) means recorded information about an identifiable individual. Fore a more detailed definition, refer to the *Municipal Freedom of Information and Protection of Privacy Act*.

- **"Remote Access Users"** are Authorized Users who have permission, by way of an authorized form with an explanation from a Senior Manager to the CFO, wherein access to the Board's internal network from a remote location outside of the normal environment regardless of the connectivity method, is provided.

- **"Systems Monitoring"** means aggregate, broad-based, or statistical data collection and review in relation to simple or multiple Users for systems analysis, planning, security, and performance purposes, or to assess, maintain, upgrade, or ensure the ongoing availability, reliability, security, confidentiality, and integrity of the Board's I&T Resources. Data collected for these purposes may include records of Internet access, including sites visited and time spent, downloads, and uploads, as well as the flow, origin, and destination of inbound and outbound e-mail. This data collection may occur routinely and regularly, or may be part of a specific audit or review activity.

- **"Unauthorized"** refers to an I&T Resource that has not been provided by the Board or an action that is not permitted by the terms of this policy.

- **"User Monitoring"** means recording, accessing, and reviewing or analyzing a User's activity on, or use of, the Board's I&T Resources, and may include review of data files, e-mails, and information sent from, received by, or stored on the Board's I&T Resources, including data, files, e-mails, and information deleted by a User but backed up by the Board's network system.

4. Policy

4.1 **General** – Authorized Users must comply with this policy. All Authorized Users are responsible for their use of the I&T Resources during business and non-business hours.

4.2 **Work Related Requirements** – All I&T Resources are to be used for Board business purposes except where otherwise stated in this policy and all such use shall be in accordance with the *Acts*.

Some work requirements may, on the surface, be in conflict with the policy. In such instances the Authorized User will obtain written authorization from the ITMT, prior to carrying out these work requirements.

Authorized Users must produce, when requested by the ITMT, any I&T Resource for required maintenance or inventory.

4.3 **Prohibited and Unacceptable Uses** – Uses of I&T Resources that are prohibited and unacceptable include, but not limited to the following:

(a) Downloading, uploading, storing, sending, distributing, or displaying messages, files or data, the contents, titles, filenames, or headings of which are unrelated to the business of the Board, including by not limited to messages, graphics files or other data that:

- are obscene, lewd, lascivious, or pornographic;
- are intended to harass, intimidate, threaten, embarrass, humiliate or degrade another employee or co-worker;
- target an individual, or groups of individuals for purposes of harassing, intimidating, threatening, embarrassing, humiliating, degrading or discriminating against the targeted individual or group of individuals on the basis of their race, ancestry, place of origin, colour, ethnic origin, citizenship, creed, sex, sexual orientation, age, marital status, same-sex partnership status, family status or disability; and
- contain defamatory references or depictions of other individuals.

(b) Sending any messages or data in a manner which violates the copyright, patent, trade secret or other intellectual property laws of Canada or any individual province.

(c) Sending chain letters or messages, whether or not the letters or messages solicit money or goods and services.

(d) Unauthorized copying, destruction, deletion, distortion, removal, concealment, modification or encryption of messages, client information, files or other data on any of I&T Resources.

(e) Unauthorized or inappropriate sending, posting or otherwise disclosing personal and or confidential or proprietary information/data of any nature of either the Board or another person or business entity with whom the Board conducts business.

(f) Accessing or attempting to access another Authorized User's computer account, e-mail or voice mail messages, file or other data without the express consent of the Authorized User or without the express direction of an authorized senior manager, except as provided for in Section 4 of this policy.

(g) Installation of any unauthorized and/or unlicensed software on any I&T Resources, including: games, shareware, freeware, screen savers (only those that can be obtained from the Board's network system is permitted), file sharing software and instant messaging.

(h) Use of the I&T Resources to make unauthorized, unlicensed and/or illegal copies of any software.

(i) Use of the I&T Resources which is in violation of any applicable federal, provincial or local law including, but limited to, the use of such I&T Resources for hacking, cracking, bugging, virus distribution, or accessing and/or tampering with government or private data without authorization.

(j) Use of the I&T Resources in any manner that violates any codes of professional conduct to which employees of the Board may be subject to.

(k) Installing software or any I&T Resources that are not owned or provided by the Board unless the ITMT authority has permitted such installation.

(l) Connecting personal or non Board-owned equipment to the Board's network without the prior written authorization of the ITMT.

(m) Adding any peripheral, internal or external, unless prior written authorization is obtained from the ITMT.

(n) Unauthorized repairing or attempting to repair any Board owned information and technology resource.

The above is not an exhaustive list of all prohibited uses. All Authorized Users are expected to carefully consider professional judgment and the actions they take prior to using I&T Resources and should contact the ITMT for advice and clarification.

4.4 **Personal Use (Limited & Occasional)**

Limited and occasional personal use of all I&T Resources is defined as follows. The usage:

- Is conducted during non-working hours including lunch time or breaks;
- Does not detract from an Authorized User's work responsibilities or job performance;

- Does not impair the normal functioning of an information and technology resource or interfere with another Authorized User's use of the I&T Resources;
- Does not result in the Board incurring an expense for such personal use;
- Is not an activity that may result in personal gain (e.g. derive income from a secondary source); and
- Is in strict compliance with the terms of this policy and other Board policies.

4.5 **Data and Records** – All information created, acquired, or maintained using Board resources including electronic messages and records are deemed to be corporate business records, property of the Board and subject to the requirements of the *Acts*.

The Board is not responsible or liable nor will it incur any expense with regards to protecting or backing up of personal files. This includes, but is not limited to: personal files that have been improperly accessed, copied, shared or lost while stored in the Board's I&T resources.

- All corporate business records are governed by retention schedules of the Board
- Authorized Users must save corporate business records on the network server, or use the "archive" function in the e-mail system to retain business-related messages**.** See: E-Mail Policy
- USB storage devices, CD burners, DVD burners must be used in accordance with applicable legislation/by-laws and only with permission from your immediate supervisor.

4.6 **Protection of Information and Technology Resources**

4.6.1 **Security** – authorized users must access Board information assets and technologies in a manner consistent with the information security principles of confidentiality, integrity and availability.

Confidentiality – data is disclosed to authorized individuals and systems on a need-to-know basis.

Integrity – data is accessed or modified by authorized individuals in line with their job responsibilities on a need-to-know basis.

Availability – data is made available for use by authorized individuals and systems. For example, users are prohibited from bypassing Board information protection controls by using software that creates security-related loopholes. Authorized Users must contact the ITMT should they suspect that their system has been compromised.

4.6.2 **Virus Protection**

Authorized Users:

- are prohibited from knowingly running, installing or sending files or messages that contain programs designed to disrupt other systems, damage or place excessive load on a computer or network. Examples: computer viruses, worms or password cracking programs;
- must exercise caution and take reasonable care when receiving e-mail messages that contain attachments, regardless of their origin, to guard against the introduction of viruses;
- must refrain from forwarding messages regarding virus warnings to other Board users but may forward them to the ITMT to investigate; and
- All instances of virus infection or suspected infection must be reported to the ITMT.

4.6.3 **Remote Access**

Authorized Users:

- must not leave a remote information and technology resource unattended or exposed while logged on to the Board's network without taking the appropriate security precautions such as workstation lockdown;
- are responsible for the privacy, confidentiality and integrity of corporate business records downloaded through their account, and must regularly delete the corporate business records downloaded to I&T Resources not owned or provided by the Board; and
- must make every effort to ensure files they transfer or upload to the Board's network are virus free.

4.6.4 **Protecting the Information Technology Resource from Illegal Access**

Authorized Users:

- must ensure that each password used to log-on to computers, telephones, mobile devices, applications, or databases remains confidential, is changed at intervals set in accordance with the requirements of the system in question, and is not left in plain sight where it can be found (e.g. taped to PC, under a keyboard). If any password is disclosed, it must be immediately changed;
- leaving their equipment unattended must log off, use screen saver passwords and/or lock the equipment, except if a resource is shared; and
- sharing a computer must log off completely and may not activate password-protected screensavers or hardware password locks.

Note- Refer to the IT support staff for instructions on how to enable/change passwords.

4.6.5 **Information Storage-Backup**

Authorized Users:

- must store all corporate information on the network server(s) to ensure proper backup; and
- are strongly discouraged from storing corporate data on removable media such as floppy disks, CDs, USB storage devices, etc.

Personal messages, files or data must be deleted and must not be kept online or archived.

5. Privacy Considerations and User Monitoring

5.1 **General Principles**

- Users should have no absolute expectation of privacy for any use of the Board's I&T Resources, whether for Board business purposes.
- The Board has an unfettered right to conduct Systems Monitoring at will and in its sole discretion.
- The Board will conduct User Monitoring in accordance with this policy.

5.2 **Technology-Related Privacy Limitations, including Systems Monitoring**

- Users are reminded that the privacy, confidentiality and integrity of e-mail and internet communication is not protected and cannot be guaranteed, due to the inherent characteristics of these uses. For more information, and guidance on best practices in use, Users are referred to the Board's E-Mail Policy;

- Users are reminded that the Board records, logs, and collects and analyzes data and information on I&T Resource use, for purposes related to system planning, analysis, expansion, upgrade, and maintenance, and to ensure the security, confidentiality, integrity, and availability of the Board's I&T Resources. These activities do not fall within the definition of "User Monitoring" in this policy, but rather, within the definition of "Systems Monitoring" set out above. The Board retains absolute discretion to perform such Systems Monitoring as it requires at any time; and
- Users should also be aware that User data and files on the Board's I&T Resources are regularly backed up and stored, and are recoverable, even if the original files, documents, e-mails, or data have been deleted by the User.

5.3 **User Monitoring**

The Board reserves the right, but does not have a duty, to perform User Monitoring, as set out below:

5.3.1 User Monitoring may be undertaken in accordance with the process outlined below, if there is a reasonable belief that the Board's I&T Resources are being used or may have been used inappropriately, in violation of this policy or of the law, or in any other fashion incompatible with the Authorized User's employment with the Board and access to the Board's I&T Resources. The reasonable belief may arise from internal or external complaint, from the results of Systems Monitoring, from personal observation, or from credible information received.

5.3.2 Where a reasonable belief arises that User Monitoring is required for the reasons set out above, the User's Senior Manager will report the situation to the CFO, including details of the basis for the reasonable belief. The CFO will review the matter and, if he/she agrees with the supervisor's recommendation for User Monitoring, will bring the matter to CEO, who may consult with the City Solicitor. If all parties consulted agree that User Monitoring is appropriate under the circumstances, the CFO will direct and supervise the User Monitoring, and present the results to the referring parties for decision.

5.3.3 The User Monitoring process set out above does not preclude recourse to external authorities, such as the Police, where merited.

5.3.4 User Monitoring may also be conducted by the Board to protect its interests, comply with legal requirements, defend itself in proceedings, or for legitimate business, corporate, or human resources purposes including as a result of the absence of an employee. The process followed by the Board in these instances will be crafted, in consultation with the CEO, who may also consult with the City Solicitor, based on the circumstances.

5.3.5 User Monitoring for personal curiosity or not in accordance with the processes set out above, is prohibited.

6. Compliance

In advance of using an Information and Technology Resource, Authorized Users should request a clarification through the ITMT if they have any concerns regarding compliance.

7. Consequences of Breach of Policy

Failure to comply with this policy may result in disciplinary action up to and including dismissal.

8. Roles & Responsibilities:

8.1 All Authorized Users are responsible for:

- Reading, understanding and complying with the Information & Technology Acceptable Use Policy

- Requesting clarification through their Senior Manager if they have any concerns regarding compliance
- Using I&T Resources responsibly and appropriately

8.2 Senior Management Team is responsible for:

- Ensuring Authorized Users have read the Information & Technology Acceptable Use Policy
- Being the first point of contact for Authorized Users to seek clarification of this policy
- Authorizing Users to access the Board's information and technology resources
- In consultation with the ITMT, authorizing exceptions to this policy for work related requirements
- Reporting suspected policy violations to the CFO, including the details of the basis for the reasonable belief

8.3 **Information & Technology Authorized Staff is responsible for**:

- Supporting the day-to-day operations of the Board such as data transfer, data backup and the installation and configuration of hardware and software

8.4 **Information & Technology Manager, as directed by the CFO and/or the CEO, is responsible for**:

- Configuring remote access to the Board's network
- Configuring designated usage of the internet
- Performing system monitoring

8.5 **CEO and CFO are responsible for**:

- On consultation of the City Solicitor, directing and supervising user monitoring and presenting the results to the referring parties for decision
- Reviewing suspected policy violations with the reporting members of the Senior Management Team

8.6 **Board's Representative re Corporate Access & Privacy is responsible for**:

- Providing advice and direction regarding the legal rights of access to information and privacy protection contained in the MFIPPA and PHIPA *Acts*

9. Related Board Policies and Applicable Legislation

Board Policies

- Conflict of Interest/Code of Conduct
- Fraud & Other Similar Irregularities
- Workplace Rules & Conduct
- Workplace Harassment

Applicable Legislation

- Canadian Charter of Rights and Freedoms
- Canadian Human Rights *Act*
- Municipal Freedom of Information and Protection of Privacy *Act* (MFIPPA)
- Ontario Human Rights Code
- Personal Health Information Protection *Act* (PHIPA)