*The Peel Centre*

# *Information Communication Technology (ICT) Policy*

Telephone Policy

Peel telecommunication services play a critical role in daily business communication. Although you may occasionally need to make a personal call at work, in general you should restrict your use of Peel telecommunications services to business.

Peel uses systems and procedures to streamline telecommunications services and reduce costs. These efforts include call detail recording, restricted services where full telephone service is not required, and investigation of abusive or fraudulent activities. To resolve confirmed instances of telecommunications abuse or fraud, Peel in its discretion may seek payment for the charges incurred or seek legal and/or disciplinary action against the offender.

Electronic Mail (e-mail)

The Peel Centre uses electronic mail to facilitate communication in the workplace. The same standards of decorum, respect, and professionalism that guide us in our face-to-face interactions with each other and with anyone outside the Centre apply to the use of e-mail.

Generally, only Peel employees, temporary employees, and on-site third party contractors are allowed to access our electronic mail system. Unauthorised access or use of this system is prohibited and may subject the violator to disciplinary action as well as civil and criminal prosecution.

Electronic files and communications created, stored or received through company systems belong to the Peel Centre. Misuse of company systems may result in restriction or termination of access privileges and other disciplinary action, up to and including termination of employment.

Company systems are supplied for business purposes. Misuse or excessive personal use of company systems is subject to management review.

The Peel maintains a right to intercept, divert, discard, access or review the contents of any email, electronic communication or file created.

Uses of email and related conduct which are strictly prohibited –

- Language that is obscene, sexually orientated, derogatory, offensive, threatening, insulting, harassing or harmful to recipients.
- Promotion of any private business venture
- Messages or stored information that are disparaging of others based on sex, race, sexual orientation, age, creed, religious or personal beliefs.
- The initiation or participation in the sending of chain letters, junk mail or other similar mailings.
- Messages that are damaging to the Peel reputation or are libellous or defamatory of any other organisation or individual.
- Unauthorised messages that represent the users personal opinion to be that of the company.

- Messages that solicit or promote a religious, political or other non-business related cause.

E-mail efficiency - Peel employees who use e-mail may receive and send many messages a day. Help make this method of communication as effective as possible by using it efficiently, responsibly, and economically.

No Auto-Forwarding - You may not establish an "automatic" forward of electronic mail to an address outside the Peel domain. For example, you may not auto-forward your work email to a personal email account with an outside provider. Doing so jeopardises Peel's confidential information by increasing the risk of the unauthorised transmission or disclosure of internal communications to unauthorised parties.

Abuse of Internet access is a violation of policy and grounds for disciplinary action up to and including termination of employment. The following uses of the Internet are specifically prohibited at all times –

- Viewing pornographic or sexually orientated web sites and downloading or distributing material from such sites.
- Viewing web sites that advocate illegal activity.
- Viewing web sites that are disparaging of others, based on race, sex, sexual orientation, age, creed, religious or political beliefs.
- Copying, distributing or using material from the Internet that may be protected by copyright or is pirated.
- Participating in chat rooms or bulletin boards for reasons unrelated to work responsibilities.
- Distributing or discussing the Peel's proprietary or confidential information without express permission from the Peel Director.
- Representing your personal opinions as those of the Peel.

Scan all downloaded, executable Internet files for viruses. You may be held responsible for any damage to Peel computing resources resulting from any virus you may inadvertently introduce if you are negligent. If you think a virus may have been released, notify the Centre Administrator immediately.

Password requirements - To deter unauthorised network access, all Peel network computers and email accounts are password protected. You should only use the password provided and should not disclose this to anyone else.

Passwords should contain at least 7 characters. They should use upper and lower case letters and at least one non-alphabetic character whenever possible. Your password should NOT include: your login name in any form (for example, reversed, doubled, or capitalised); your first, middle, maiden, or last name; the name of your partner, child, pet, or any other word conveying easily obtainable information about you or a name or word pertaining to Peel.

Monitoring - The Peel Centre respects your privacy. We do not monitor e-mail arbitrarily. In certain circumstances, however, Peel may review electronic mail accounts. For example, system administrators may see the contents of messages in the

course of performing their duties. If warranted, Peel may monitor electronic mail systems to investigate internal misconduct or if email policy is being violated. Such access must always be authorised by the Peel Director.

Hardware and Software

All additions of hardware or installations of software to Peel computer systems must be approved by the Peel Director. Under no circumstances should any computer have software installed without express permission. The Administrator is responsible for ensuring an up to date inventory of equipment and software is maintained and should be consulted on all aspects of updating or upgrading.

Saving Information to Peel Computer Systems

The procedure for saving information is that there are one master set of folders. These are contained on the ‘host’ machine. All information as far as possible (unless only relevant to a specific department) should be saved in these folders. A comprehensive list of folders in existence on the ‘host’ machine is attached. Please choose carefully and ensure that the file name is incorporated on each document produced in order for easy access. If at any time you are unsure as to where to save documents please speak to the Administrator.