Information Technology Usage Policy

1. Preface

"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the community."

Background and Purpose

This document constitutes a council-wide policy for the appropriate use of all MDC computing and network resources. It is intended to provide effective protection of individual users, equitable access, and proper management of those resources. These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts which currently apply to those resources.

Access to MDC networks and computer systems is granted subject to Council policies and Government laws. Appropriate use should always be legal and ethical, reflect academic honesty and community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms; and individuals' rights to privacy, freedom of speech, and freedom from intimidation, harassment, and unwarranted annoyance.

The Council is not responsible for unacceptable or unethical use of the information technology environment including computer and computer networks or electronic communication system.

2. Appropriate Use

Appropriate use of information technology resources includes instruction; independent study; authorized research; independent research; and official work of the offices, units, and all recognized departments of the Council.

Authorized use of MDC-owned or operated computing and network resources is consistent with the education, research, and service mission of the Council, and consistent with this policy.

Authorized users are: (1) staff of the Council; (2) anyone connecting from a public information service; (3) others whose access furthers the mission of the Council and whose usage does not interfere with other users' access to resources. In addition, a user must be specifically authorized to use a particular computing or network resource by the Head of Department/Unity responsible for operating the resource.

Acceptable conduct in and use of this environment must conform with: existing Council policies, guidelines, and codes of conduct

Therefore, any misuse or violation of MDC's information-technology environment will be judged in accordance with those published policies and rules of conduct, including, but not limited to Workers Standing Order.

It is your responsibility to be aware of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to continuously verify the integrity and completeness of information that you compile or use. You are responsible for the security and integrity of Council information stored on your individual computing desktop system.

3. Confidentiality and Privacy

Authorized access to data or information entails both privilege and responsibility, not only for the user, but also for the system administrator. In general, the council will treat information stored on computers as confidential. However, there is no expectation of privacy or confidentiality for documents and messages stored on Council-owned equipment. Additionally, e-mail and data stored on MDC's network of computers may be accessed by the council for the following purposes:

a. troubleshooting hardware and software problems,
b. preventing unauthorized access and system misuse,
c. retrieving business related information,*
d. investigating reports of violation of this policy or local, state law,*
e. complying with legal requests for information,*
f. rerouting or disposing of undeliverable mail.

* The system administrator will need specific approval from the Head of ICT and Relation Unity or the appropriate designee to access these items. The extent of the access will be limited to what is essentially necessary to acquire the information.

To the greatest extent possible in a public setting individuals' privacy should be preserved. However, privacy or confidentiality of documents and messages stored on Council-owned equipment cannot be guaranteed. Users of electronic mail systems should be aware that, in addition to being subject to authorized access, electronic mail in its present form cannot be secured and is, therefore, vulnerable to unauthorized access and modification by third parties.

4. Examples of Prohibited Use

Use of MDC network and computer systems is conditioned upon compliance with this and other council policies and all applicable laws. Though not exhaustive, the following list is provided to emphasize that these activities are NOT allowed on MDC networks or computer systems:

a. using departments, accounts, access codes, privileges or information for which you are not authorized;
b. ***sharing your password with others;***
c. viewing, copying, altering, or destroying anyone's files without explicit permission from that individual;
d. representing yourself electronically as another user;
e. unlawfully harassing others;

f. creating and/or forwarding chain letters;
g. posting or mailing obscene materials;
h. game playing that interferes with administrative use by others;
i. making, distributing, or using unauthorized copies of licensed software;
j. unauthorized copying, reproducing, or redistributing others' text, photos, sound, video graphics, designs or other information formats;
k. obstructing others' work by consuming large amounts of system resources, such as disk space, CPU time and etc.;
l. unauthorized testing of systems and/or resources, such as using program loops, introducing destructive software e.g., "virus" software or attempting system crashes;
m. running or otherwise configuring software or hardware to intentionally allow access by unauthorized users;
n. attempting to circumvent or subvert any system's security measures;
o. advertising for commercial gain;
p. distributing unsolicited advertising;
q. disrupting services, damaging files or intentionally damaging or destroying equipment, software or data belonging to MDC or other users;
r. using computing resources for unauthorized monitoring of electronic communications;
s. destroying public records;
t. violating any MDC or government law.

In cases of doubt, users bear the burden of responsibility to inquire concerning the permissibility of external network uses, prior to execution. Such questions should be directed to the Head of ICT and Relation Unity.

5. Reporting Violations

All users and units should report any discovered unauthorized access attempts or other improper usage of MDC computers, networks, or other information processing equipment. If you observe, or have reported to you, a security or abuse problem, with any Council computer or network facilities, including violations of this policy, you should notify the Head of ICT and Relation Unity, the District Executive Director or other appropriate administrator.

6. Sanctions

Persons in violation of this policy are subject to the full range of sanctions, including the loss of computer or network access privileges without notification, disciplinary action, dismissal from the Council, and legal action. Some violations may constitute criminal offenses, as outlined Cybercrime Act; the Council will carry out its responsibility to report such violations to the appropriate authorities.

Department/Unit heads have the authority to deny access, for unauthorized use, to MDC's computers and network systems under their control.

7. Effective Date 01/07/2014