

1.0 POLICY STATEMENTS:

- 1.1 The use of electronic mail (e-mail) as a communication and transfer of information medium is provided by the University to authorized employees, students and affiliates for business use; and,
- 1.2 The content of Electronic mail is a “record” under the Freedom of Information and Protection of Privacy Act and the Records & Information Policy D7220. It must be managed in the same way as any other record of the University.

2.0 REGULATIONS:

- 2.1 Electronic mail communication is intended for official business use. Employees should apply the same kind of discretion in their use of electronic mail as they would with respect to other department sources such as telephones, fax machines and photocopiers.
- 2.2 Grant MacEwan University reserves the right to access all files stored on its systems, all information within application files and all messages transmitted over its systems. All such access must be logged by the network administrator and any such action taken should be monitored by the FOIP Coordinator.
- 2.3 Grant MacEwan University will not conduct general or secret monitoring of employees regarding the content of electronic mail except for law enforcement purposes; or, with the approval of an officer of the University, where allegations of inappropriate use have arisen.
- 2.4 All collection, use and disclosure of personal information involving the electronic mail system will be done in accordance with the requirements of Part Two of the Freedom of Information and Protection of Privacy Act.
- 2.5 Employees must ensure the security of their use of electronic mail service by ensuring the integrity of their password.
- 2.6 Employees are prohibited from willfully destroying any records, including electronic mail records with the intent to evade a request for access to the records (section 92(1)(g) of the Freedom of Information and Protection of Privacy Act).
- 2.7 Employees should not transmit over the electronic mail system any information which could reasonably be expected to cause an unwarranted invasion of privacy of an individual and would normally be held confidentially by Grant MacEwan University.

- 2.8 In accordance with the Records and Information Management Policy and procedures, employees are responsible for properly filing and disposing of electronic mail; for ensuring appropriate content in messages they send; for making messages accessible to others as business requires; for taking reasonable precautions to ensure the integrity, confidentiality and security of information transmitted over electronic mail systems; and for appropriate dissemination of their electronic mail messages.
- 2.9 Employees who do not comply with this Policy may be subject to restriction or suspension of electronic mail privileges or disciplinary action, depending upon the seriousness of non-compliance.

3.0 PROCEDURES:

- 3.1 All employees are responsible for appropriate filing and retrieval of official electronic mail and all attachments, particularly mail containing formal approval, authorization, delegation, or handing over of responsibility, or similar transactions, which must be printed and placed in the appropriate hard copy file in accordance with the File Classification System. Transitory electronic mail should not be filed on network drives and should be disposed of in a timely manner.
- 3.2 Annually, or at such time as hard copy and other records are being disposed of (transferred to semi-active or inactive storage, sent for shredding, etc.) the department responsible for a certain electronic folder will dispose of the electronic files within that folder, in accordance with established retention and disposition schedules.
- 3.3 Official (non-transitory) electronic mail must be retained and disposed of in accordance with the University records management policies and any approved retention and disposition schedules.
- 3.4 Any official records in the electronic mail system may be included in a request for information under the Freedom of Information and Protection of Privacy Act.
- 3.5 Employees may be asked to search their e-mail box in order to locate information pertinent to a request.
- 3.6 Until the request has been dealt with and all review periods have expired, no e-mail pertinent to a request may be destroyed even where approved schedules are in place.

3.7 E-mail Protocol – Employees must ensure that messages:

- all official electronic mail must include the address, recipient, distribution, transmission and receipt information;
- are accurate and courteous (once sent, a message cannot be retracted);
- are sent to selected employees with a need to know;
- protect others rights to privacy;
- do not illegally harass or disparage others (e.g. sexually explicit messages, racial or ethnic slurs);
- do not violate the copy right of others (when in doubt, get permission), and
- includes a signature block with name of sender and e-mail address if sending messages externally. When sending e-mail for another person, signature block should say message sent by “x” for “y”.

4.0 DEFINITIONS

4.1 Electronic Mail

Electronic mail means the electronic transfer of information typically in the form of electronic notes and memoranda amongst and between Grant MacEwan University employees and employees of other organizations with whom Grant MacEwan University has a business relationship.

4.2 Official Electronic Mail

Official Electronic mail contains a record of a decision or other official action or a way of documenting business activity (formal approval, authorization, delegation or handing over of responsibility, or similar transactions) and must be printed and placed on the appropriate hard copy file including all attachments.

4.3 Transitory Electronic Mail

Transitory Electronic mail has only temporary usefulness; isn't part of an administrative or operational records series; is not regularly filed in a records system; and is required only for a limited time to complete a routine action and may be deleted under the authority of the originator and receiver.

FACT SHEET

DATES:

Approval	99.04.15
Review	2004.04

SOURCE:

99.04.15	New policy approved by Board Motion 1-4-15-98/99.
2003.02.01	Format updated.
2009.10.08	Terminology updated to reflect name change to Grant MacEwan University. Approved by Board motion 01-10-8-2009/10

APPENDIX “A”

The following types of information have been identified as requiring additional safeguards:

- a) Third party business information or trade secrets, including commercial, financial, scientific, technical or labour relations information, supplied explicitly or implicitly in confidence and who disclosure would be expected to significantly harm the third party.
- b) Personal information (as defined in section 1(n) of the Freedom of Information and Protection of Privacy Act).
- c) All information in Personal Information Banks as listed under GMC in the Alberta Directory (1995) or any subsequent version of the directory.
- d) Information whose disclosure would be harmful to individual or public safety.
- e) Information whose disclosure would be harmful to individual or public safety.
- f) Information whose disclosure would reveal local public body confidences.
- g) Information whose disclosure would reveal advice from officials (which could include program or outcome evaluations).
- h) Information whose disclosures would be harmful to the economic and other interests of GMC.
- i) Information relating to testing or auditing procedures or techniques or details of specific tests to be given or audits to be conducted.
- j) Information that is subject to any type of legal privilege, including solicitor-client privilege.

APPENDIX “B”

Related Policies and Procedures

1. Records and Information Management Policy, D7220 – Establishes guidelines and responsibilities for the creation, organization, management, security, continuity, handling, storage, scheduling and disposition of information identified as a record.
2. Electronic Mail Policy, D7225 (Under Development) – Establishes general guidelines and responsibilities for the appropriate use, management, filing, retention, and disposition of electronic mail.
3. Use of University Computer Facilities and Information Resources, D6010 – Promotes the responsible, ethical and secure use of the University’s computing facilities and information resources.
4. Internet/Intranet Policy (Needs to be Developed).
5. Disposal of Electronic Data Storage Devices (Needs to be Developed).