Policy Number	9.6
Approval Body	Executive Committee
Policy Officer	Director ITS
Approval Date Review	August 2009 2012

9.6 INFORMATION PROTECTION

ENABLING LEGISLATION + LINKED POLICIES

Freedom of Information and Protection of Privacy Act

OBJECTIVE

The objective of this policy is to ensure the collection, use, retention, disclosure and security of administrative data is lawfully maintained, and to assure faculty, staff and students that privacy and confidentiality matters have been considered in the design, implementation and management of Emily Carr University of Art + Design (University) information systems.

The University recognizes that such information assets are valuable and critical to running the University, but can be vulnerable to misuse and loss.

SCOPE

This policy applies to administrative data which is data generated by/for administrative functions of the University such as Finance, Human Resources, Facilities, Information Technology Services (ITS), Student Services, University Advancement, Technical Services and other administrative functions. Administrative data may include confidential and/or personal information.

This policy applies to faculty, staff, students and third parties who may create, use, store or disseminate administrative data on behalf of the University.

While this policy is directly relevant to information stored in an electronic format, it is intended to guide users of all types of information. This policy applies to data and information captured at source, as well as copies that may be made and stored separately from source data.

POLICY

1. Collection, use and storage of administrative data should occur only where there is a legitimate and justifiable business need and in a controlled manner. A legitimate need arises within the scope of University employment or in the performance of authorized University-related duties.
2. Administrative data will be identified with appropriate retention cycles established.

3. Administrative data will be destroyed in an appropriate and timely manner once past the retention date and when it is no longer serving an administrative or historical need.

4. Administrative data will have appropriate access controls, limiting access to authorized individuals based on their role or job function within the University. All administrative information systems developed, purchased or used by the University will provide functionality to adequately control access to data.

5. Senior leaders of each functional administrative area are responsible for ensuring access to administrative data related to their area is adequately controlled, retained and secured.

6. The following are examples of unacceptable behavior that are contrary to this policy:

    a. Changing or disclosing information about yourself or others in an unauthorized way, or for individual gain (this does not apply to “self-serve” applications that are designed to permit a user to change information about themselves);

    b. Engaging in “administrative voyeurism” such as tracking salary raises, monitoring telephone calling patterns, or looking up grades unless authorized to perform such analysis;

    c. Facilitating another individual’s illegal access to our administrative data.

7. At all times, users of administrative data will remain mindful of applicable laws and University policies related to handling and disclosure of such data.

8. Suspected violations of this policy should be reported to ITS. Disciplinary measures may be taken in accordance with applicable regulations, agreements, laws and University policies.

9. ITS may deploy and utilize tools to track and monitor the handling and disclosure of administrative data. These tools may operate in a manner that is not visible to end users of information systems. Data created by or stored in these tools is considered administrative data and subject to the terms of this policy.