OLDS COLLEGE			
POLICY			
Olds College recognizes the need for Policies and Procedures, and the need for staff and students to be familiar with and follow such policies and procedures. It is the policy of the Board of Governors that breach of College Policies or Procedures shall result in disciplinary measures up to and including suspension or termination. This applies to all College staff and representatives.			
CATEGORY:	E. Information and Technology Management		
SUBJECT:	Privacy, Information Security, and Identity Management		
POLICY NUMBER:	E02		
CROSS REFERENCE:	A18 Access and Protection of Privacy E01 ITM Governance and Management		
NEW \ REVISED			
Board of Governors	Administrative Services Committee	Academic Council	Common Issues
Date: June 27, 2013	Date: June 18, 2013	Date:	Date:

POLICY STATEMENT

Protecting privacy, securing information and managing identity are critical responsibilities assigned to and accepted by all information users of Olds College**.**

Rationale

Information is at the core of and enables the Institution's business processes. Protecting privacy, securing information, and managing identity is critical to ensure:

- Compliance with legislation, regulations and contractual requirements
- Understanding and incorporation of these concepts into the design, implementation and evolution of programs, systems and services as well as daily practices
- Information is regarded and managed as a valuable asset that must be protected throughout its lifecycle in accordance with its criticality, confidentiality, and value
- Trust between Olds College and its information users is maintained
- Individual rights and values are upheld by providing them with choice of service delivery channels, obtaining their informed consent and empowering them to control their own identity to the extent possible
- Access is secured proportionately to the assessed risk
- Accuracy and integrity is maintained
- Activities and decisions are open, transparent, and understandable

Scope

This policy applies to all information assets, regardless of media, and processing infrastructure. Protection, security and identity management efforts must be proportionate to the sensitivity of the information and the assessed risk.

SPECIFIC GUIDELINES

Relevant Legal Instruments

Acts and Regulations that authorize or influence this policy include, but are not limited to:

- Alberta Evidence Act
- Alberta Centennial Education Savings Plan Act in whole and specifically sections 4, 6(a) and (h)
- Alberta Centennial Education Savings Plan Regulation in whole and specifically sections 2, 3 and 5
- Apprenticeship and Industry Training Act specifically section 50(2)
- Certification of Teachers Regulation enacted pursuant to the School Act
- Code of Conduct enacted pursuant to the Public Service Act
- Electronic Transactions Act
- Freedom of Information and Protection of Privacy Act (FOIP)
- FOIP Regulation enacted pursuant to the FOIP Act
- Financial Administration Act
- Government Emergency Planning Regulation enacted pursuant to the Emergency Management Act
- Health Information Act (HIA)
- Historical Resources Act
- Records Management Regulation enacted pursuant to the Government Organization Act
- Personal Information Protection Act (PIPA)
- Post-secondary Learning Act, specifically sections 65 and 118

Related Content

None

Supporting Control Objectives for IT (COBIT) 4.1 Control Processes

DS5 – Ensure System Security
DS12 – Manage the Physical Environment

COBIT 4.1 Control Process Exemptions

None

Measurement

Internal and external audit findings regarding these controls:

- User Account Management
- Identity, Authentication, and Access Management
- Physical and Environmental Security

- Information Security and Classification

IMPLEMENTATION AND ADMINISTRATIVE RESPONSIBILITY

Vice President, Student and Support Services in consultation with the Director, Information Technology.

This policy will be reviewed at least every 5 years.