RED RIVER COLLEGE
OF APPLIED ARTS, SCIENCE AND TECHNOLOGY

ITI

Policies and Procedures

Acceptable Use of Information Technology Resources

Originator: Information Technology Governance Committee
Approver: President's Council
Effective: October 16, 2007
Replaces: A20 – Acceptable Use of Computer Facilities October 1, 1997

1. Preamble

The vision of Red River College is "to be recognized as a leader through the innovative use of technologies." To that end, Information Technology Solutions (hereinafter IT Solutions) will "make a positive contribution to meet the goals of the College Community by working collaboratively with the Community to deliver quality service and solutions that meet the current needs and changing requirements."[1]

In turn, the use of College information technology resources imposes responsibilities and obligations on the Users of these resources. Users must maintain an environment in which access to all information technology resources is shared fairly among users and is conducive to teaching and learning.

The College will ensure that all assets, including information technology resources, are protected, adequately maintained and not subject to unnecessary risk."[2]

2. Policy

Red River College information technology resources will be used to support the administrative, teaching, learning, research and community services goals of the College.

Users of information technology resources will act responsibly and must respect the rights of other Users, the integrity of the system and related physical resources. They must observe all relevant College Policy, Federal and Provincial law, regulations and contractual obligations.

The College believes that it has a social responsibility to provide leadership and follow community standards with respect to the distribution and use of offensive materials. The College has a zero tolerance for these inappropriate activities.

A normal expectation of privacy cannot be guaranteed to a User of College information technology resources.

[1] IT Strategic Plan Executive Summary
[2] Board of Governors Policy Manual

3. Definitions

3.1 Information Technology resources (hereinafter IT resources) are defined as, but not limited to:

a. computer equipment and computer facilities
b. networks, including wired and wireless, networking and communications equipment, cabling infrastructure, and access to and usage of College networks
c. User accounts and passwords usage and information access privileges
d. data files, data storage devices and servers
e. computer applications, software and services
f. internet access and usage
g. email access and usage
h. data records, computer software, documentation and media

3.2 Users are students, staff and external clients with whom the College maintains a business relationship. It also includes the general public in public access locations.

4. Procedures

4.1 By accepting a College information technology account, Users accept the responsibilities of this Policy and the consequences of failure to comply. Users must read and abide by the intent and content of this Policy. Their acceptance is implicit by the use of their account.

Breach of Policy

4.2 Instructors and supervisors will provide a warning to students or staff of a breach of this Policy.

4.3 Repeated or serious violations by staff are to be reported to the individual's supervisor and to IT Solutions.

4.4 Repeated or serious violations by a student are to be reported to the student's program head and to IT Solutions.

4.5 College Security Services and authorities outside the College may report suspicious, harassing or other unacceptable use of IT resources to IT Solutions.

4.6 IT Solutions will investigate all reports. This investigation may include, but is not limited to, such methods as tracking of network activity, review of email transactions and review of the contents of all data storage devices that are attached to or part of College-owned equipment. The investigation will be documented as appropriate.

4.7 Based upon initial findings, the Director – IT Solutions or the Supervisor – Information Protection and Compliance may authorize immediate suspension of the individual's access privileges.

Unacceptable Use

4.8 The following examples include, but are not limited to, activities that are specifically prohibited under this Policy:

a. Using or accessing another User's system, files, email or other data without that User's permission unless authorized by the College
b. Attempting to circumvent security facilities on any system or network or failing to keep security current on College owned equipment
c. Attempting to compromise the integrity of any IT resources including the placement of any destructive or nuisance programs such as viruses or worms
d. Engaging in any activity that may be harmful to any IT resources
e. Unauthorized monitoring of network transmissions and general network traffic on College networks
f. Sending fraudulent, harassing, threatening or obscene messages, or sending unauthorized bulk (spam) email
g. Transmitting commercial advertisement, solicitations or promotions for any other commercial purposes not authorized by the College
h. Displaying, transmitting, distributing or making information available that expresses or implies discrimination or an intention to discriminate
i. Intentionally accessing, downloading or collecting obscene material in which the dominant characteristic is "the undue exploitation of sex, or of sex and any one or more of the following subjects, namely, crime, horror, cruelty and violence."[3] Obscene material by law has no legitimate artistic, literary or scientific purpose and as such is not protected by the freedom of speech
j. Permitting another User to use one's College information technology accounts and passwords
k. Intentionally breaching the terms and conditions of a software licensing agreement
l. Attaching unauthorized equipment to the College network including, but not limited to, personal routers, switches, hubs, or wireless access points

Non- College Related Use of Information Technology Resources

4.9 Users may use their computers and network accounts for non-College matters except where such use would be prohibited by this or other College Policy or where such use unreasonably interferes with administrative and academic uses, job performance, or system performance and operation.

4.10 Use of information technology resources for commercial and business purposes is prohibited except for those activities sponsored or sanctioned by the College.

[3] *Criminal Code*, R.S.C. 1985, c. C-46, S. 163(8)

5. Responsibilities

5.1 **Information Technology Solutions** has the right and the responsibility to monitor the use of IT resources and traffic across the network. They have the responsibility to manage, and possibly restrict, such use as required to ensure acceptable use as defined in this Policy. Information Technology Solutions is also responsible for:

a. the safety, integrity and security of the College's information technology resources
b. coordinating the investigation of alleged unauthorized use of the College's information technology resources under the authority of the Vice President - Finance & Administration or designate
c. providing current security information and anti-virus updates to the College community and automatically installing those updates where possible
d. periodically informing the College community of current procedures to be followed to ensure the integrity of the College information technology resources

5.2 **Users** of IT resources provided by the College are fully responsible for their use of these resources and for the information they willfully or knowingly transmit, receive or store. User's of the College's IT resources are also responsible for:

a. using resources for authorized purposes as defined by this Policy
b. protecting their user account and password from unauthorized use
c. selecting and maintaining strong and effective passwords
d. all activities performed by their user account that originate from their system with their knowledge
e. accessing only information that is their own, that is publicly available, or to which they have been explicitly granted access by the College for the purpose of performing their job or assignment
f. using legally licensed versions of copyrighted software or copies of documents and media in compliance with the terms and conditions of any vendor licensing agreement, copyright, or sales terms and conditions
g. engaging in ethical and respectful behaviour in the use of information technology resources

5.3 **College Instructional Staff** are responsible to enforce compliance with this Policy in the classroom. Instructors have the responsibility to report serious or repeated breaches of this Policy to the program head and IT Solutions.

6. Consequences

Persons who violate this or other related Policy may be subject to disciplinary action up to and including dismissal or expulsion as outlined in College Policy and Collective Agreements. Unacceptable use may result in the immediate loss of account privileges and access to information technology resources. Additionally, dependant on circumstances, they may face civil action and/or criminal prosecution. Disciplinary action may be appealed under appropriate Policy or the MGEU Collective Agreement.

Related Policy and documents:

IT Strategic Plan Executive Summary, Deloitte Inc. March 2006

2.12	Asset Management – Executive Limitation Board of Governors Policy Manual
H1	Respectful College
S1	Student Code of Rights and Responsibilities
S2	Student Discipline
S3	Student Appeal – Non Academic Decisions

MGEU Collective Agreement