

OLDS COLLEGE POLICIES AND PROCEDURES MANUAL

CATEGORY: **A. General**

SUBJECT: **Acceptable Use Policy
Telephone, Computing and Network Resources**

POLICY NUMBER: **A21**

APPROVALS New/Revision

Board of Governors (Policy Approval)	Academic Council	Academic Coordinating Committee	Administrative Services Committee	Common Issues (Authority)
Date: 2007/06/28	Date:	Date:	Date: 2007/06/18	Date:

POLICY STATEMENT

The telephone, computing and network resources (resources) of Olds College are the property of Olds College and are provided to enhance the learning environment and work productivity.

The purpose of this policy is to provide guidelines regarding restrictions to the use of the College's resources.

SCOPE

The policy applies to staff, students, contractors, guests and the general public. It covers all telephone, computing and network equipment owned or leased by Olds College or any equipment attached to the College's systems or network.

Resources include but are not limited to:

1. Internet/Intranet/Extranet related services
2. Computer equipment
3. Software
4. Operating systems
5. Storage media
6. Network accounts providing e-mail, WWW browsing and file transfer protocol
7. Telephones and wireless devices
8. Other related technologies

GUIDELINES

1. The data and information contained on the College's resources is the property of Olds College unless specified otherwise under an authorized agreement.
2. Periodic and limited personal use of resources is permitted. The College retains the right to limit this personal use. Individuals are prohibited from using the resources for personal commercial use or in a manner that violates the Harassment Policy.
3. Confidential corporate material located on the Internet/Intranet/Supernet must be protected. This includes but is not limited to student or staff information, financial information, research data and sensitive corporate information.
4. With the exception of devices used through wireless connections, new hardware and software can be added only with the approval of IT staff.
5. With the exception of devices used through wireless connections, computer equipment can be moved only with the approval of IT staff.
6. IT staff are required to periodically audit networks and systems. This process may result in accessing data resident on the network and related hardware.
7. All users are responsible for keeping their passwords and accounts secure. System passwords are changed every 3 months. Reuse of passwords is prohibited.
8. All PC's, laptops and workstations connected to the College network will be password protected or will log-off automatically after a set period of inactivity. Automatic log-off time intervals will be established to ensure appropriate system security.
9. Due to the capability of forwarding, opinions expressed when using the College email system should reflect the best interest of the College and relate to the sender's area of responsibility. This includes emails to newsgroups or listservs.
10. Any equipment or device connected to the College network must be continuously running approved virus-scanning software. The Information Technology Department is responsible for documenting authorized virus-scanning software.

UNACCEPTABLE USES

See Appendix A. Changes and additions to Appendix A are approved by Olds College Executive.

E-MAIL GUIDELINES

See Appendix B. Changes and additions to Appendix B are approved by Olds College Executive.

ENFORCEMENT

Olds College reserves the right to copy and examine any files or information resident on College systems allegedly related to unacceptable use and to protect its network from systems and events that threaten or degrade operations.

Failure of staff to comply with Olds College Policy may result in disciplinary action being taken in accordance with the Counseling and Discipline Policy. Failure of students to comply with Olds College Policy may result in disciplinary action being taken in accordance with the Student Academic/Behavioral Status Policy.

IMPLEMENTATION AND ADMINISTRATIVE RESPONSIBILITY

Director, Information Technologies and Library Services. This policy will be reviewed every 3 years.