STANDARD	ACCEPTABLE USE
Owner: **Information Technology**	Approved Date: **11 November 2024**

SUMMARY

This Standard outlines the acceptable use for individuals utilizing Olds College of Agriculture & Technology (Olds College) provided computer equipment and is in place to protect both the user and Olds College. The use of these resources is a privilege that is extended to members of the College community. As a user of these services and facilities, you have access to valuable College resources, to high risk and/or moderate risk information, and to internal and external networks. Consequently, it is important for you to behave in a responsible, ethical, and legally compliant manner.

Inappropriate use of computer equipment exposes Olds College to risks including cyber attacks, compromise of network systems and services, availability of services and bandwidth in the pursuit of the organizational goals and legal issues. This Standard enforces the principle of defense in depth and monitoring the effectiveness of security controls, while ensuring compliance with organizational, legal and regulatory requirements.

Information Technology has the responsibility to ensure appropriate practices are adopted to conform to this Standard and the Information Security Policy that it supports.

APPROVAL

Approved by:	Joe Guenther	**Position:**	Director, Information Technology
		Date:	22 May 2024
Approved by:	Peter Mal	**Position:**	VP, Student Experience
		Date:	11 November 2024

SCOPE

All users, students, employees, contractors, consultants, third party business associates, volunteers, temporary/other workers and the Board of Governors at Olds College must adhere to this Standard as it applies to the use of the digital assets of the organization.

AUTHORITY

This Standard has been created under the authority of Olds College E01 Digital Security Procedure which maintains the right to ensure that this Standard is adhered to.

ENFORCEMENT

Any Olds College user found to have violated this Standard may be subject to disciplinary action, including restriction of and possible loss of network privileges or more serious consequences, up to and including suspension, termination, or expulsion from the College. This policy supplements other Olds College policies, including the Employee and Student Codes of Conduct, and the consequences or disciplinary processes set out in those policies also apply to this Standard. Any violation of the Standard by a temporary worker, contractor or vendor may result in, but not limited to, the termination of their contract or assignment with Olds College. As obligated by provincial and federal laws, Olds College will notify appropriate law enforcement agencies when it appears that any applicable laws have been violated.

EXCEPTIONS

A request for exception to this Standard must be submitted for approval to the Director of Information Technology by following the process as described in the Digital Security Exception Request Procedure. Granted exceptions will be for up to a one-year term and will be reviewed annually at which time the exception may be revoked, revalidated or extended for another one-year term. Exceptions will be maintained by Information Technology.

STANDARD

1. General

1.1. Data contained on Olds College's digital assets is the property of Olds College unless otherwise expressly stated.

1.2. Olds College provides computing/IT resources to students, employees and authorized guests in order to effectively operate the College and provide appropriate education support and services.

1.3. Using college computing/IT resources for any private or commercial purpose other than those sanctioned by the college in writing, is strictly prohibited.

1.4. Users are permitted to use Olds College computing resources for limited personal purposes provided that they exercise good judgment and such use is lawful and does not injure, harm or tarnish the image, reputation and/or goodwill of Olds College and any of its users; and, provided that such use does not violate the college code of conduct, interfere with the performance of their regular duties, or disrupt college operations.

1.5. The College retains the right to limit personal use at its discretion.

1.6. Computing equipment and electronic devices provided by the College, and e-mail accounts and addresses provided by the College are the property of the College. The College reserves the right to access all College computing and information systems and records, including email records, where there are reasonable grounds to believe that those systems and/or records contain information necessary to the proper functioning of the College's business and/or where the College is legally required to do so and/or to investigate compliance with College's policies and Standards. Wherever practicable, affected persons will be notified promptly when their systems and/or records have been accessed.

1.7. The use of College computing resources that facilitate criminal or fraudulent activities may subject the sharer to legal consequences.

2. User ID's/Identity

2.1. Sharing of credentials with other people, 3rd parties is strictly prohibited.

2.1.1. Students found to be sharing credentials for the purpose of cheating may be considered in violation of policies **D31 - Academic Integrity**,

2.2. Individual users of Olds College computing/IT resources are responsible for all activities performed under their assigned user identity.

2.3. Users shall not attempt to mask, obscure or falsify their identity or utilize an unauthorized identity while using Olds College computing/IT resources.

2.4. Impersonating a college employee or student by using their e-mail address or electronic signature is strictly prohibited.

3. Endpoints

It is prohibited for the user to (without explicit permission in writing):

3.1. change or alter, in any way, registry settings or system files;

3.2. set-up file sharing or Peer-to-Peer services (e.g. Bittorrent or other similar technologies);

3.3. activate any form of Personal Area Network (PAN) on their local desktop or computing device;

3.4. store music, videos or other copyrighted materials that have not been sanctioned/purchased or otherwise authorized for use by the College on their local desktop or network; (Refer to Policy A29 Use of Copyright Material for further detail.)

3.5. connect any unauthorized networking technology to their workstation, laptop or wired network ports;

3.6. leave their endpoint device logged in and unlocked if the device is unattended; or,

3.7. intentionally introduce malicious programs onto college computing/IT devices (e.g., viruses, worms, Trojan horses, e-mail bombs, key-loggers, etc.).

3.8. relocate, disassemble, alter or add unauthorized technology to classroom or meeting room technology.

3.9. block or disable any installed college security functions.

4. Network

It is prohibited for the user to (without explicit permission in writing):

4.1. modify assigned network settings to gain access to computer resources and/or data;

4.2. use network inspection/scanning/capture technologies without written permission;

4.3. intentionally introduce malicious programs onto the network (e.g., viruses, worms, trojan horses, e-mail bombs, key-loggers, etc.).

4.4. introduce unauthorized computing devices onto college networks; or,

4.5. obtain configuration information about a network or system for which the user does not have administrative responsibility.

5. Software

5.1. Software that has been licensed to Olds College for business use must not be installed on personal equipment without the express prior approval of the Director of Information Technology or designate.

5.1.1. Microsoft or Adobe software may be available via the IT Department for staff & students for installation on their personal devices during their tenure / studies at Olds College.

5.1.2. Staff who work remotely will be provided with Olds College computing devices and software required for their College work.

5.2. All software protected by copyright must not be copied except pursuant to a valid license or as otherwise permitted by copyright law.

5.3. The number and distribution of software copies must be handled in such a way that the number of simultaneous users does not exceed the number of licenses purchased, unless otherwise stipulated in the purchase contract.

5.4. In addition to software, all other copyrighted material (text, images, icons, programs, videos, music, etc.) must be used in conformance with applicable copyright law and legitimately copied material must be properly attributed.

5.5. Users shall not break or otherwise circumvent Technical Protection Measures (TPM's) or any other security on software or other digital materials used at the college.

6. E-mail & Electronic Communications

6.1. The provisioning of Olds College e-mail is to accomplish the mission of the organization and will be used for such purposes.

6.2. Before opening e-mail attachments, users must be certain of their source. If the source is unknown or cannot be verified, users should call the Service Desk for assistance.

6.3. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material is prohibited and may be in violation of Canada's Anti-Spam Legislation (CASL).

6.4. Creating or forwarding "chain letters", or other "pyramid" schemes, of any type is prohibited.

6.5. Making a political comment by institution email is prohibited.

6.6. E-mail, or any sort of electronic communication content should reflect the values of Olds College and therefore should not be of a questionable, obscene or inappropriate nature, or convey any information that could be injurious to the institution.

6.7. E-mail, or any sort of electronic communication must not jeopardize the institution's commitment to confidentiality and security of information.

6.8. All e-mail must follow institutional standards regarding protection of privacy and security of information and attachments.

6.9. The Service Desk must be notified immediately when the source of an e-mail is unclear, where harm towards Olds College or possible threat to the digital security of the college is suspected.

6.10. The use of the Olds College email account for personal matters or personal business that may cause reputational or financial harm to the institution is prohibited.

6.11. The user must not use personal email to conduct business on behalf of Olds College.

7. Internet

Web browser access is strictly prohibited to sites that:

7.1. poses a risk to the security and performance of the college network;

7.2. potentially incur legal liability to the institution or the individual user;

7.3. damages the institution's reputation, or;

7.4. violates the Code of Conduct or College Values.

7.5. Sites that may be blocked and/or monitored for access are:

7.5.1. banner ad service sites;

7.5.2. web-based chat sites or services;

7.5.3. hacking sites;

7.5.4. violent or offensive sites;

7.5.5. cloud based storage sites or services;

7.5.6. remote proxies;

7.5.7. gambling sites;

7.5.8. sites containing pornographic, adult or sexually explicit material;

7.5.9. sites where content is illegal (breach of criminal law); and,

7.5.10. sites that are otherwise deemed to be incompatible with our Code of Conduct and Values.

7.6. The use of Olds College resources to store, display, or disseminate child pornography or hate crimes is strictly prohibited. As obligated by provincial and federal laws, Olds College will notify appropriate law enforcement agencies when access to child pornography or hate crime web sites has occurred.

7.7. College computing resources must not be used for the creation, transmission, storage, access or viewing of materials which in any way contribute, support or promote actions which are prohibited on the basis of harassment and/or discrimination including but not limited to the categories of: Harassment, Sexual Harassment, Pornographic, Racial/Ethnic/Cultural Harassment, Discrimination, Hate Literature, Systemic Harassment/Discrimination & Reprisal

7.7.1. This restriction is not intended to interfere with legitimate and appropriate uses for teaching purposes.

7.7.2. This restriction does not apply to the investigation of above mentioned actions and/or materials.

8. Information Handling / Data Access

8.1. Users shall not attempt/access college data that is beyond their expressed approved permissions.

8.2. Users shall not modify/remove data or files owned by someone else without written permission.

8.3. All college data or records are to be stored on Olds College owned or approved network drives and shall **NOT** be stored on local drives (on your PC, laptop or other digital device) or unapproved cloud based services to ensure appropriate backup and data custody can be maintained.

8.4. Users must ensure that files containing confidential data are stored in appropriately secure locations.

8.5. All storage devices such as CDs, USB memory sticks, Smartphones, cell phones, laptops and other removable media containing institution data must be securely maintained by the user. This means that the device shall be either kept in your possession or locked in a storage location like an office filing cabinet, lockable desk drawer or safe when not in use.

8.6. While in transit, institution data storage devices should be secured as noted in the Data Transmission Standard.

8.7. Users must take appropriate precautions to ensure that college information is only disclosed to individuals authorized to receive that specific information.

8.8. It is strictly prohibited to take individually identifiable information or records from Olds College's facilities or systems to your residence or another non-work environment. This includes:

8.8.1. student records;

8.8.2. Olds College systems, business or research records;

8.8.3. health related information;

8.8.4. user records; or,

8.8.5. anything that includes personal information unique to an individual.

8.9. IF sensitive data is taken from Campus for the purpose of remote work, all necessary precautions need to be taken to ensure the security and privacy of that information.

8.10. Users must not save any Olds College related information contained in documents or e-mail communication to their home or other computers.

8.11. Files being worked on by a user must not be e-mailed to their home, sent to a personal e-mail address for access outside of the work environment or copied to some form of personal removable digital media.

8.12. If users must work on files at home, the primary method is accessing the files via the Virtual Private Network (VPN) connection while working from an Olds College laptop. Google Drive / Docs / Sheets or the College's Remote Desktop Gateway service (nimbus.oldscollege.ca) can be used when working from their personal computer.

8.13. All files must be scanned for malicious software before being loaded onto institution networks, storage devices, workstations or laptops.

9. Instant Messaging (IM)

9.1. Google Chat functions as the institution approved Instant Messaging platform for internal business use. What'sApp private one-to-one Messaging, especially with International Students recruitment and application processing, is also institution approved.

9.2. The disclosure of sensitive, private, confidential College information via public IM networks (group chat, discussion forums) is prohibited.

9.3. The use of Social Media Platforms (e.g. Instagram, TikTok, Facebook, Twitter, LinkedIn) as per A42 Social Media Policy for official College communications is permitted.

9.4. Parties to a conversation may save a copy of the IM conversation.

9.5. The exchange of user credentials (usernames and passwords together), confidential or personally identifiable information in an IM session is prohibited.

9.6. Sending messages that could be interpreted as being improper or injurious to Olds College, such as junk, spam or chain messages, or information relating to pyramid schemes over IM is prohibited.

9.7. All Google Chat or Microsoft Teams conversations may be monitored and/or logged for investigation purposes.

10. Service Desk Laptops (loaner laptops)

10.1. All files copied to Service Desk Laptops (SDL's) must be removed before the SDL is returned to the Service Desk.

10.2. Before configuring a SDL for network access (for example, VPN), users must obtain Service Desk approval.

10.3. Users must not load software onto SDL. The Service Desk must approve and load all software onto an SDL.

10.4. All SDL's must be returned the day they are expected. Special authorization from the Service Desk must be obtained for extending SDL sign-outs past their due dates.

11. Smart Phones

11.1. Users are permitted to install approved applications from trusted sources (e.g. Google Play or iTunes) on their institutionally issued Smartphone, provided the applications do not impact institutionally installed applications.

11.2. The user is reminded, in relation to data that may be stored on your Smartphone, that it is strictly prohibited to take individually identifiable information or records from Olds College's facilities or systems to your residence or another non-work environment. (NOTE: Business contact information is not considered individually identifiable information under privacy legislation).

11.3. Users must not attempt to disable any of the security features as provisioned (or updated from time to time) by Olds College or jailbreak the devices.

11.4. Users issued an Olds College Smartphone are responsible for the security of the device regardless of where the device is used (for example, in the office, at a user's place of residence or in any other location such as a hotel, conference room, car or airport).

11.5. The camera functions on Olds College issued Smartphones are available for users to use; however, taking photos or video of Olds College data is strictly prohibited.

11.6. Any smartphone that is configured to connect to Olds College emails or documents, must be password, PIN, or authentication protected at the lock screen.

DEFINITIONS

1. **Commercial Gain** - A gain, usually financial in nature, accruing to the benefit of a business/corporation or other entity either registered or unregistered, not to the benefit of the college.
2. **Computing/IT Resources –** An electronic set of technological tools and resources used to communicate, and to create, disseminate, store, and manage digital information.
   Olds College computing resources include all information systems, computers and computing equipment, owned by and/or operated by or on behalf of the College, as well as data owned by and/or operated by or on behalf of the College whether that data is accessed or used on College-owned equipment or on personal devices.
3. **Digital Asset –** Any electronic device used to access Olds College Data.
4. **Jailbreak** – modify (a smartphone or other electronic device) to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorized software.

5. **Junk Mail** - unwanted or unsolicited advertising or promotional material received through the mail or by email.
6. **Network inspection/scanning/capture technologies** – are software or hardware devices that capture network packets or frames that are used on the communications network of Olds College.
7. **Peer-to-Peer** - denoting or relating to computer networks in which each computer can act as a server for the others, allowing shared access to files and peripherals without the need for a central server.
8. **Private Gain** - A gain, usually financial in nature, accruing to the benefit of an individual, not to the benefit of the college.
9. **Technical Protection Measures (TPM)** - include technology that provides digital locks preventing individuals from undertaking a variety of actions, such as copying, printing or making alterations, or controlling viewing; and, often operate alongside Rights Management Information associated with copies of works that usually identify the owner or author of the work and define the types of permitted access and/or track usage.
10. **Virtual Private Network (VPN)** - is a network that is constructed over a public network — usually the Internet — to connect remote users or regional offices to a company's private, internal network. A VPN secures the information using encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. This type of network is designed to provide a secure, encrypted tunnel in which to transmit the data between the remote user and the company network, and thus the name “Virtually” private network.
11. **Public IM Networks** - Public chat or discussion forums such as, but not limited to, Reddit, Discord, Facebook Groups & Messages, What’sApp Group Messages,