Policy

INFORMATION AND COMMUNICATION TECHNOLOGY USAGE POLICY

Policy Section & Number:			**Effective Date:**	
Policy Owner:	Vice President Infrastructure & CIO		**Last Revised:**	N/A
Policy Administrator:	Associate Director Information Technology		**Review Scheduled:**	4 Years
Approver:	Executive Committee			
The official controlled version of this document is held with the Policy & Procedure Coordinator.				

A. POLICY STATEMENT

The purpose of this policy is to define Keyano College's expectations and requirements for the use and management of the College information technology resources.

1. Guiding Principles

1.1 Keyano College information technology resources are to be used primarily for activities related to the mission of the College, including, but not limited to teaching, learning, research and administration.

1.2 Limited personal use (i.e., use not related to the mission of the College) is permitted provided it complies with this Policy, does not compromise the business of Keyano, does not increase the College's costs, does not expose Keyano to additional risk, does not damage Keyano's reputation, and does not unduly impact the College's business and academic uses. All other uses are prohibited.

1.3 Information Technology resources must be used and managed in a responsible manner. Use of these resources for disruptive, fraudulent, harassing, threatening, obscene (including but not limited to racist, profane, and pornographic in nature), or malicious purposes is strictly prohibited. Use of information technology resources for personal commercial purposes is prohibited unless authorized by the appropriate Dean or Director.

1.4 Users must respect intellectual property, copyrights, and licenses to software, entertainment materials, published and unpublished documents, and any other legally protected digital information.

1.5 Application and enforcement of this policy shall be in accordance with the College Intellectual Property and Ownership Policy.

1.6 Use of College information technology resources, including electronic identities, is permitted only to members of the College community, and authorized guests.

1.7 Information technology resource users must stay within their authorized limits and refrain from seeking to gain unauthorized access to information technology resources beyond their permissions and privileges.

1.8 Any individual using information technology resources to create, access, transmit or receive College-related information must protect that information in a manner that is commensurate with its value, use, and sensitivity.

1.9 Users must respect the rights of other users. They must not encroach on other users' rights to use, access, and privacy.

1.10 All forms of electronic communication are expected to reflect high ethical standards and mutual respect and civility. Users must refrain from transmitting to others, inappropriate images, sounds, or messages which might reasonably be considered harassing, fraudulent, threatening, obscene (e.g., pornographic), defamatory, or other messages or material that are a violation of applicable law or College policy.

1.11 Users must be sensitive to the open nature of public spaces (for example, computer labs and classrooms) and take care not to display in such locations images, sounds or messages that are harassing, threatening, obscene (e.g., pornographic), defamatory, or that are a violation of applicable law or College policy.

1.12 The College will protect information against unauthorized disclosure. The College reserves the right to access, monitor and record both stored or in-transit data and the usage of information technology resources when there is suspected or alleged impropriety, a business need for access in the absence of an employee, a request under the Freedom of Information and Protection of Privacy Act, or as otherwise required by law. The College has the right to use information gained in this way in disciplinary actions as prescribed in College policies, and to provide such information to appropriate internal and external investigative authorities.

1.13 Anyone witnessing or suspecting an information technology security incident and/or unacceptable use of College information technology resources in a manner that contravenes this Policy, is obligated to respond and report in accordance to the Data Breach of Security Procedures.

Support and assistance can be obtained through the IT Helpdesk at 780-791-4965 or itshelpdesk@keyano.ca.

1.14 The College reserves the right to withhold and revoke access to its information technology resources to any individual if there are reasonable grounds to suspect that their continued access to the resources poses a threat to the operation of the resource or the reputation of the College.

1.15 The College's actions under this policy will be taken in accordance with the Code of Conduct and the Safe Disclosure Policy.

1.16 System administrators of information technology resources have the responsibility to investigate and act in the case of suspected or alleged unacceptable use. With the approval of their supervisor and with due regard for the rights of users' privacy and the confidentiality of users' data, system administrators have the right to suspend or modify users' access privileges to information technology resources. System administrators have the responsibility to take immediate action in the event the College is at imminent risk. System administrators may change passwords, examine files, accounting information, data, and any other material that may aid in an investigation of possible abuse.

1.17 Non-compliance with this policy constitutes misconduct and may be handled under the applicable collective agreements, College policy, or law.

B. DEFINITIONS

(1) Automatic Email Forwarding: Configuring one's College email account (@keyano.ca) to automatically forward incoming emails to a non-sanctioned external third party.

(2) College: Means Keyano College.

(3) Electronic Identity: An electronic identity is any means by which a person may be identified and authenticated to access an information technology resource. This includes, but is not limited to, an account name and password, encryption keys, proximity cards, swipe cards, smart cards, biometric devices (fingerprint readers, facial identification, etc.), or other forms of identification.

(4) Information and Communication Technology: A term that describes various IT technologies inclusive of desktops, laptops, mobile phones, desk phones and Microsoft Teams, etc.

(5) Information Technology Security Incident: Means events where there is suspicion that:

- the confidentiality, integrity, and availability of College data has been compromised,

- information and information technology resources are used for, or violated by, illegal or criminal activity, and/or
- information technology resources have been attacked, is currently under attack, or is vulnerable to attack.

(6) Information: Data, or aggregate data, created using College information technology resources.

(7) Policy: means the Information and Communication Technology Usage Policy.

(8) System Administrator: System Administrator refers to the person or persons responsible for configuring, installing, maintaining, and supporting information technology resources for the College. A System Administrator of an information technology resource may also be a user of that resource.

(9) User A user is defined as an authorized person who utilizes a College computer or network service. Users can consist of Students, Staff, Contractors and Community members.

C. RELATED POLICIES

- Data Breach of Security Policy
- IT Password and Authentication Policy and Procedure
- Intellectual Property and Ownership Policy
- Non-Academic Misconduct Policy
- Progressive Discipline Policy
- Code of Conduct
- Safe Disclosure Policy
- Protection of Privacy Policy

D. RELATED LEGISLATION

- *Freedom of Information and Protection of Privacy Act*
- *Criminal Code of Canada*
- *Alberta Health Information Act (HIA)*

E. RELATED DOCUMENTS

- Appendix A - Email Forwarding Restriction
- Appendix B - Examples of Unacceptable Use

F. REVISION HISTORY

Date (mm/dd/yyyy)	Description of Change	Sections	Person who Entered Revision (Position Title)	Person who Authorized Revision (Position Title)
February 2021	NEW	All	Associate Director IT	Vice President Infrastructure & CIO

Appendix A

EMAIL FORWARDING RESTRICTION

Staff are not permitted to enable automatic email forwarding to external email addresses. Automatic email forwarding to external third parties and providers prevents the College from maintaining custody and/or control of its information and records. This responsibility is mandated by legislation such as the Freedom of Information and Protection of Privacy Act (the Act) of Alberta. Email forwarding places Keyano College information and records at risk as the controls, safeguards, and assurances required and in place with the College's standard email service are not present with other external third parties.

College information and records shall not be automatically email forwarded.

Responsibilities

Members of the Keyano College community are responsible for protecting College information and records.

Faculty and staff, and other stakeholders working with College information and records shall not configure their College email account settings to automatically forward to external third-party providers, which places information/records at risk and out of reach from Keyano's access and control.

Students and alumni are not bound to this procedure mandate as their email communications do not typically involve College information and records.

Exceptions

1. The only accepted exceptions to the email forwarding restriction are those cases assessed and approved by the Vice President Infrastructure & CIO, and Associate Director Information Technology.
2. Requests for exceptions to the College email forwarding restriction appendix will be submitted to the Associate Director IT.

Non-compliance

Non-compliance with this Appendix constitutes misconduct and may be handled under the applicable collective agreements, College policy or law.

Appendix B

EXAMPLES OF UNACCEPTABLE USE

The following are some examples of unacceptable use of information technology resources, as referenced in the Information and Communication Technology Usage Policy. The list is not comprehensive but is meant to serve as a guide for the type of activities that are not permitted.

A. Unauthorized Access
Unauthorized Access includes password or account sharing, attempts to gain unauthorized access to computer accounts, or any activity designed to bypass an installed computer or network security mechanism. Such activities are contrary to the Information and Communication Technology Usage Policy as well as the Criminal Code of Canada, or other applicable legislation. Note, authorized delegate access to a specified and limited set of resources (such as an email calendar), is permitted, provided the required approvals and restricted permissions as related to job function, are in place.

B. Excessive Resource Consumption
Excessive resource consumption includes excessive network or computer resource use for personal or commercial reasons, such as peer-to-peer file sharing. Excessive resource use contravenes the Information and Communication Technology Usage Policy, as this use interferes with the operation of networks and systems.

C. Copyright or License Violations
Copyright or License violations include installing, reproducing, or distributing copyrighted materials such as any software, publications, or electronic content without permission. Installed software and media on College networks is provided under license agreement and may not be copied or removed without permission. Users may not use College information technology resources to use, modify, or redistribute third party copyrighted data or software that they do not have specific approval to use, modify, or redistribute. These violations contravene the Information and Communication Technology Usage Policy and may contravene legislation and legal agreements.

D. Theft of data, Unauthorized Disclosure, or Modification of Data
Deliberate unauthorized alteration or unauthorized destruction of computer files is an offence under the Criminal Code of Canada. The inspection, altering, deleting, publishing, copying, or modification of any data an individual is not authorized to access is prohibited. Violations of this nature also contravene the Information and Communication Technology Usage Policy.

E. Vandalism
Vandalism in this context includes vandalism of data, denial of service (DOS) attacks, or any behavior which intentionally degrades, modifies, or adversely impacts the behavior of any computer or network system, for any reason. This includes interfering with another individual's work. Violations of this nature contravene Information and Communication Technology Usage Policy and other College policy and procedures.

F. Unauthorized Commercial Use

Unauthorized commercial use contravenes the Information and Communication Technology Usage Policy and other College policies. One example of unauthorized use is running an unauthorized corporate web presence on a College server.

G. Objectionable Content

The use of obscene, racist or sexist language, or public displays of pornography, clearly violate the ethical standards of the College community and is as inappropriate for electronic communication as it is for other forms of College discourse. Such use contravenes the Information and Communication Technology Usage Policy, other College policies, and may contravene legislation as well.