FANSHAWE

COLLEGE POLICY MANUAL

Policy No. & Title:	**C202: ACCEPTABLE USE OF COLLEGE TECHNOLOGY**
Effective:	2022-03-31
Next Review:	2027-03-31
Policy Sponsor:	Chief Information Officer
Approvals:	2000-05-03/SA-99-09; 2001-02-07/SA-00-04; 2001-10-03/AC-01-01; 2008-09-10/AC-08-01; 2012-02-08/SLC-11-07; 2015-07-14; 2022-03-31

1. PURPOSE

The purpose of this policy is to establish a framework for the acceptable use by employees, and other authorized users, of College computing and communications resources and services (“College technology”).

2. POLICY

College technology is provided to support the learning, teaching, research, enrichment and administrative needs of the College. Use of these resources must be responsible, ethical, and lawful at all times. The use of College technology for personal gain or profit, including but not limited to the operation of any personal business, is prohibited.

Occasional use of College technology for personal purposes is acceptable provided it does not: interfere with the primary uses of the technology; impose incremental costs or degrade performance; pose a security risk to the College; or contravene College policy or applicable legislation.

The Policy Sponsor develops, maintains and Implements standards and guidelines that achieve the objectives of this policy. Such standards and guidelines align with the College mission, vision and strategic goals, and reflect best practices and College values.

3. REFERENCES

College Policy A204 Copyright

4. ADDENDA

Guideline A: ACCEPTABLE USE OF COMPUTER RESOURCES
Guideline B: ACCEPTABLE USE OF VOICEMAIL AND EMAIL

-0-0-

Policy No. & Title: C202: ACCEPTABLE USE OF COLLEGE TECHNOLOGY

Addendum: **Guideline A: ACCEPTABLE USE OF COMPUTING RESOURCES**

Issued by: Chief Information Officer

Effective: 2022-03-31

1. PURPOSE

The purpose of this guideline is to establish College expectations regarding the use by employees and other authorized users of the computing resources and infrastructure owned or managed by the College. Safe and secure computing practices are essential to maintain the integrity and security of the College's information and to protect the College, its students and employees. The College expects employees to utilize the College computing resources and infrastructure for the conduct of College-related business. Use by students of the College computing resources and infrastructure is subject to the Student Code of Conduct and such other policies as may apply.

2. DEFINITIONS

College computing resources and infrastructure: Includes personal computers, laptops, tablets, Smartphones, printers, related peripherals, servers, software, electronic storage, networks and virtual services that are owned, operated, managed or licensed by the College.

Computer virus: Programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document.

Confidential information: Information, regarding any College-related activity, that is not otherwise available to the public and that has been created, communicated or received by or within the College with the expectation that it remains confidential.

Malware: Malicious software, programs or files that are designed to damage, disrupt or access a computer or system without the owner's consent. Examples are viruses, worms, key loggers, spyware, logic bombs, back doors and Trojan horses.

Personal information: (Per Section 2(1) of the Ontario Freedom of Information and Protection of Privacy Act) Recorded information about an identifiable individual, including:

- Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;
- Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
- Any identifying number, symbol or other particular assigned to the individual;
- The address, telephone number, fingerprints or blood type of the individual;
- The personal opinions or views of the individual except where they relate to another individual;

- Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;
- The views or opinions of another individual about the individual; and
- The individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

3. GUIDELINES

3.1. Computing resources and infrastructure support the learning, teaching, research, enrichment and administrative requirements of the College. Use of these resources must be responsible, ethical, and lawful at all times. Employees have a duty to ensure that their computer practices do not adversely affect others or expose personal or confidential information to inadvertent disclosure, theft or loss.

3.2. The use of College computing resources and infrastructure for personal gain or profit, including but not limited to the operation of any personal business, is prohibited.

3.3. The College reserves the right to access and manage all information stored on or transmitted within the College computing infrastructure. Notwithstanding that the College permits occasional incidental personal use of its computing resources (as outlined below), information stored within the College's computing infrastructure, including personal information in individual accounts and e-mail, is the property of the College. While it does not routinely do so, the College may monitor computer and Internet use, including reviewing materials stored in individual accounts and emails or on College computers or other devices, to ensure that such use is consistent with this policy, the purposes, goals and policies of the College, and with relevant legislation and regulations.

3.4. Occasional use of College technology for personal purposes is acceptable provided it does not: interfere with the primary uses of the technology; impose incremental costs or degrade performance; pose a security risk to the College; or contravene College policy or applicable legislation.

3.5. All computing activities are conducted so as to protect the integrity and security of College systems and data. In this regard:

3.5.1. It is important for employees to use secure computing passwords containing at least eight digits and typically containing a combination of letters (upper and lower case), numbers and symbols. Personal passwords are never shared by account holders.

3.5.2. Computers used to access College computing resources and infrastructure must have up-to-date anti-virus protection and operating system patches.

3.5.3. Smartphones, tablets and other wireless-connected devices used to access College computing resources and infrastructure must have password protection enabled

3.5.4. Lost or compromised passwords must be reported to the IT Service Desk immediately

3.5.5. Employees are required to report the loss or theft of College computers, Smartphones, etc. to the IT Service Desk, their supervisor, campus security services and local authorities where appropriate, as soon as possible

3.5.6. Employees should lock out or log off their computers when they are not at their workstations.

3.5.7. Employees are required to notify their supervisors in the event of any known or suspected breach of security, loss of information, or introduction of a virus or malware into the College's computing infrastructure or network

3.5.8. Encryption is used when transmitting personal or confidential information over electronic public networks such as the Internet.

3.5.9. Where an employee's work requires personal or confidential information stored on portable or laptop computers or portable storage devices, (e.g., USB drives) the information must be encrypted so as to protect against inadvertent disclosure in the event of loss or theft.

3.5.10. Installation of unauthorized software or hardware for the purpose of breaching security, capturing electronic passwords or communications, conducting security scans or extending the network is prohibited.

3.6. Employees comply with copyrights, patents, intellectual property laws, contractual obligations and license agreements that may apply to software, files, graphics, documents and articles. Material downloaded from the Internet may be subject to copyright or otherwise restricted and all such material is subject to College policy A204: Copyright.

3.7. Unless otherwise approved, e-mail communication with students is conducted using College-provided or College-sanctioned e-mail services. This enables continuity of student-professor communications should it be necessary for a substitute professor to assume responsibility for a course or section during an academic term.

3.8. The written authorization from a College Budget Manager is required prior to permitting any third party to access College computing resources.

3.9. Responsibility for Content

3.9.1. Each employee bears the primary responsibility for the materials they send, access, or display. This responsibility applies equally to the use of College computing resources and to the use of such innovations as blogs, social networking sites and wikis. Users must respect the public nature of the College, and refrain from sending, posting on electronic bulletin boards, accessing, downloading, disseminating, printing or displaying any images, sounds, messages, or depictions which could reasonably be expected to be offensive, or harassing, or which could reasonably be seen as detrimental to the interests of the College.

3.9.2. The use of College computer resources and of innovations such as blogs, social networking sites and wikis must be consistent with the *Ontario Human Rights* Code and other applicable laws, and with this policy and other College policies.

3.10. Corporate directories and information stored on College servers are routinely managed and backed up to protect against systems failure, unauthorized access and data loss. Wherever possible, where an employee's work requires personal and confidential information to be stored, it should be stored on corporate servers. Individuals are responsible for ensuring work contained on personal computers is appropriately backed up and safeguarded against unauthorized access, use disclosure or destruction.

3.11. Employees must ensure that all e-mails and other electronic communications are written in a professional and businesslike style.

3.12. Responsibilities

3.12.1. Employees are required to adhere to this policy and are accountable for their actions. Supervisors are responsible for monitoring compliance within their areas of responsibility.

3.12.2. A breach of this policy or other misuse of the College computing resources may result in disciplinary action up to and including termination of employment or financial restitution to the College.

3.12.3. Authorized users of the College computing resources who are not employees of the College are subject to this policy.

-0-0-0-

Policy No. & Title: C202: ACCEPTABLE USE OF COLLEGE TECHNOLOGY
Addendum: **Guideline B: ACCEPTABLE USE OF VOICEMAIL AND EMAIL**
Issued by: Chief Information Officer
Effective: 2022-03-31

1. PURPOSE

The purpose of this document is to establish customer service procedures and standards for College employee use of voicemail and email services.

2. PRINCIPLES

College telephone and email services are established to be primary mediums for employee communication with internal and external College communities and others with whom the College conducts business. The information and impressions that employees present through these services may either enhance or detract from the reputation of the College.

The guidelines below describe how employees are to use voicemail and email services so as to best serve the interests of the College on a consistent basis. College employees comply with this policy by following the procedures and by meeting the standards described in the appendices. Supervisors monitor employee use of voicemail and email service and take action as necessary to ensure compliance.

A - EMPLOYEE USE OF COLLEGE VOICEMAIL

Effective use of voicemail is a key tool for the achievement of quality customer service at Fanshawe College. The following are mandatory procedures and standards for employee use of College voicemail services. These standards apply to employees having dedicated voicemail service associated with their College telephone number or extension.

1. Greeting Message Currency

   To be useful, voicemail greeting messages must be current, complete and accurate, and must convey useful information in concise format. Messages not meeting these basic criteria do a disservice to our customers and are not acceptable.

   Your voicemail greeting is normally changed each working day with information concerning your schedule and availability during the day. However, a simple "I am in the college today" message is acceptable so long as the message is changed when you are not in.

2. Greeting Message Content

   Voicemail greetings contain information concerning your College affiliation (School, Campus, department, etc.), the day and date, and your availability during office hours. When another person is acting for you, provide their contact information in your greeting message. Similarly, absence from the College is noted together with information concerning who to contact in urgent situations and when you expect to respond to voicemail messages.

3. Private Messages

   When people call a personal extension at the College, they generally expect to speak with the person listed for the extension. If you have a business need for someone else to answer your extension, be certain that the person receiving your calls is able to forward the caller to your voicemail should the caller wish to leave a personal or confidential message for you.

4. Individual or Shared Voicemail Box

   Individual voicemail boxes are intended to be confidential to the owner. Do not share an individual voicemail box, or have others take messages from it on your behalf, unless you indicate in your greeting that others may access your messages. Where a voicemail box is shared among employees, the voicemail greeting will indicate that the mailbox is shared.

5. Forward to Voicemail

   Call-forwarding to voicemail (if available) is used when you are temporarily away from your phone during the working day. As well, call-forwarding to voicemail is to be engaged when you depart for the day. By so doing, you show respect for your callers' time by not requiring them to listen through multiple rings before reaching your voicemail when you are not available.

   Note also that it is preferable to allow messages to go to your voicemail rather than to forward them to an extension that may not be answered. For example, do not call-forward to an assistant who might be photocopying or on a break.

6. Standard for Response to Voicemail

   Except in instances where your voicemail greeting makes it clear to the caller that you are unable to do so, voicemails that require a response are answered normally within one business day. Incoming voicemail messages are to be checked and cleared on a timely basis that achieves this response time standard.

   If you are away from the College for an extended period and unable to check your voicemail, indicate in your greeting that you are unable to access messages and state when you expect to be able to do so.

   Failure to respond to voicemail messages is not an acceptable business practise.

7. Screening Calls

   College telephone services are provided to facilitate communication. Use of voicemail to avoid answering calls or to screen calls is not an acceptable business practice.

8. Sample Voicemail Scripts

   8.1 Hi, you have reached the voicemail of Mary Smith in the Facilities Services department at Fanshawe College. Today is Wednesday, January 21, and I am scheduled to be in the College throughout the day. I will be in meetings for most of the afternoon. I'm sorry that I've missed your call and I hope that you will leave me a message, together with your number, and I will return your call as soon as possible. If your call is urgent, please call our department receptionist at 519-452-xxxx, extension xxxx for assistance.

   8.2 Hello, this is Mary Smith of the General Studies Division at Fanshawe College. It's Wednesday, January 21, and I'll be out of the office all day today without access to voicemail. I will be returning to the College tomorrow. If you'd like to leave me a message after the tone, please do so, and I will get back to you when I return. Let me know how I can be of assistance to you, and please leave a return number where you can be reached. If you require immediate assistance, please call our Division receptionist at 519-452-xxxx, extension xxxx

8.3 Hi, you've reached the confidential voicemail of Mary Smith in Human Resources at Fanshawe College. I am on holidays from Wednesday, January 21 through Friday, January 23. While I am away, Jean Brown will be acting for me. Jean can be reached at 519-452-xxxx, extension xxxx. If you'd like to leave me a message with your number, please do so, and I will get back to you when I return.

9. Voicemail Best Practice

When leaving messages in the voicemail boxes of people you have called, provide your telephone extension number and subject. This courtesy saves them having to spend time looking up your number and allows them to prepare before returning your call.

B - EMPLOYEE USE OF COLLEGE EMAIL

Effective use of email is a key tool for quality customer service at Fanshawe College. The following are mandatory procedures and standards for employee use of College email services. Please contact the IT Service Desk (x4357) for assistance with email features mentioned below.

1. Acceptable Use

   College email services include Microsoft Outlook/Exchange and Fanshawe Online email systems. These systems are provided to support the achievement of College objectives and are the property of the College. Refer to Guideline A of this policy for further guidance.

2. Anti-Spam Compliance

   Electronic messages sent by Fanshawe employees must conform to Canada's Anti-Spam Legislation (CASL). Express or implied consent of all intended recipients is required for the dissemination of any commercial electronic messages. All such messages must also contain information about the sender as well as an unsubscribe mechanism.

3. Faculty Email Communication with Students

   Faculty members are required to use FanshaweOnline for email communication with students.

4. Email Security

   Email traveling through the Internet is subject to interception by unintended parties: any email containing sensitive or confidential material must be encrypted to avoid inadvertent disclosure. The IT Service Desk can offer advice and assistance with security and encryption technologies.

5. Standard for Email Response

   The College standard for responding to business email is normally one business day. In some situations, a shorter response time is appropriate.

6. Standard for Email Signature Block

   A signature block with your name, position, organization (i.e., your School, department, etc., and 'Fanshawe College'), postal address, telephone number(s), and email address is a mandatory part of outgoing email. This courtesy gives email recipients the information necessary to contact you without having to search for your coordinates. Signature blocks can be programmed once for inclusion in all messages including those sent from college smartphones and tablets. The IT Service Desk pages on myFanshawe outline the steps to create signature blocks.

7. Standard for Email Subject Field

   Ensure that the 'Subject' field of your email contains a relevant reference when composing your messages. This is important because some email filtering products discard messages that do not have an entry in the subject field.

8. Out of Office Email Message

   If using Outlook email and you will be away from their place of work for a day or longer you are required to use the 'Out of Office Assistant' to advise those who send email to you that you are unavailable. This ensures that those attempting to contact you regarding an urgent matter will be advised of your absence.

9. Email Folder Housekeeping

   Be sure that your email box is able to receive email at all times. This requires routine maintenance by eliminating unnecessary messages. The 'Inbox', 'Sent' and 'Deleted' folders all need to be maintained since all Outlook folders consume space. Contact the IT Service Desk if you need assistance with this maintenance.

10. Email Best Practices

10.1. Email is used extensively in attempts to fraudulently acquire passwords, credit card numbers, SIN numbers or financial or personal information from account holders – a practice referred to as 'phishing.' Messages may be forged to appear from trusted sources or technical support personnel requesting account information. Recipients are sometimes requested to click on links for additional information or to 'unsubscribe.' Be wary of potential phishing attacks; avoid clicking on links and forward any suspicious messages to the IT Service Desk for assessment.

10.2. To prevent the group's email addresses from being disclosed and potentially copied or harvested by spam agents, avoid divulging email addresses to others outside the College. If forwarding email to a group or distribution list, place the distribution addresses in the 'Bcc…' (blind carbon copy) field. Similarly, consider deleting addresses in the 'Cc…' (carbon copy) field from messages being forwarded outside the College.

10.3. Reduce unwanted spam email by avoiding posting your email address on Internet forums, chat rooms, bulletin boards or other public areas.

10.4. Be selective in using the 'Reply All' feature and the 'Cc…' (carbon copy) feature. Only respond to those who expect or require a response.

10.5. Do not use attachments for short messages that can be placed in the body of an email. Instead, cut and paste text from your word processing program into the email message. This eliminates the need for recipients of your message to open a word processing program on their computers to view the attachment. As well, since not all attachments are legible on mobile devices, pasting your message in the body of the email is more reliable.

-0-0-0-