

Faculty and Staff Communications Suite Terms of Use

The Communications Suite is a package of related systems and services built around a Microsoft Exchange environment which provides a complete solution for e-mails, calendaring, task management and contacts for the Faculty and staff of Algonquin College.

The objectives of this document are to outline appropriate and inappropriate use of Algonquin College's e-mail systems and services in order to minimize disruptions to services and activities, and to comply with applicable policies and laws.

Scope

This document applies to all e-mail systems and services owned by Algonquin College, all e-mail account users/holders at Algonquin College (both temporary and permanent), and all College e-mail records.

Account Activation/Termination

E-mail access at Algonquin College is controlled through individual accounts and passwords. Each user of Algonquin College's e-mail system is required to review the terms of use document prior to utilizing an e-mail access account and password. It is the responsibility of the employee to protect the confidentiality of his or her account and password information.

All employees of Algonquin College will receive an e-mail account.

E-mail accounts may be granted to third party non-employees on a case-by-case basis. Non-employees that may be eligible for access include:

- Contractors, Independent Contractors, Temporary Agency Employees or approved individuals who require an account to conduct business with Algonquin College.

Applications for these temporary accounts must be submitted to 5555@algonquincollege.com

E-mail access will be terminated when the employee or third party terminates their association with Algonquin College, unless other arrangements are made. Algonquin College is under no obligation to store or forward the contents of an individual's e-mail inbox/outbox after the term of employment has ceased.

Retirees will be transitioned to a separate mail system. The retiree's College mail account and data will be removed within 1 month of the effective date of retirement from the College's Communications Suite

General Expectations of End Users

The College delivers official communications via e-mail. As a result, employees are expected to check their e-mail in a consistent and timely manner so that they are aware of important College announcements and updates, as well as for fulfilling business and role-oriented tasks.

E-mail users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to unsubscribe from the list, and is responsible for doing so in the event that their current e-mail address changes.

E-mail users are expected to comply with normal standards of professional and personal courtesy and conduct.

Appropriate Use

Employees and users of the College Communications Suite are encouraged to use e-mail to further the goals and objectives of Algonquin College. The types of activities that are encouraged include:

- Communicating with fellow employees, business partners of Algonquin College, and clients within the context of an individual's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Participating in educational or professional development activities.

Inappropriate Use

E-mail use at Algonquin College will comply with all applicable laws, all Algonquin College policies, and all Algonquin College contracts.

The following activities are deemed inappropriate uses of Algonquin College systems and services and are prohibited:

- Use of e-mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- Use of e-mail in any way that violates Algonquin College's directives, policies, , or administrative orders, including, but not limited to the following College Directives:
 - A8 Harassment/ Discrimination
 - A11 Freedom of Information
 - A16 Acceptable Use of the College Computer Network and Accounts
 - A21 Rights, Freedoms, Responsibilities and Code of Conduct for the Algonquin College Community
 - A25 Information Security
 - E19 Confidentiality of Student Records
 - E32 Faculty Consultation with Students
- Viewing, copying, altering, or deletion of e-mail accounts or files belonging to Algonquin College or another individual without authorized permission.

- Sending of unreasonably large e-mail attachments. The total size of an individual e-mail message sent (including attachment) should be 1000 Kb or less.
- Opening e-mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- Sharing e-mail account passwords with another person, or attempting to obtain another person's e-mail account password.
- Excessive personal use of Algonquin College e-mail resources. Algonquin College allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. Algonquin College prohibits personal use of its e-mail systems and services for unsolicited mass mailings, non-Algonquin College commercial activity, political campaigning, dissemination of chain letters, and use by non-employees. Email records arising from personal use, however may be subject to presumption of inclusion in the College's definition of corporate records. Email users should assess the implications of this presumption in their decision to utilize the College's email system for personal purposes.
- College employees will not employ a false identity when utilizing the Communications Suite. Furthermore email users will not give the impression that they are representing, giving opinions or otherwise make statements on behalf of the College unless appropriately authorized.
- Forwarding messages to external mail accounts: College mail messages are expected to be sent and received from College email accounts and so Algonquin College employees are expected to utilize the College Communications Suite for this communication. Forwarding and responding College communications to external providers or systems is not allowed without the permission of the employee's manager, in consultation with the College's Chief Information Officer (CIO).

Monitoring and Confidentiality

Algonquin College maintains the right to monitor any and all e-mail traffic passing through its e-mail system as required.

Monitoring may include, but is not limited to, review by the ITS staff during the normal course of managing the e-mail system, review by the legal team during the e-mail discovery phase of litigation, observation by management in cases of suspected abuse.

In addition, archival and backup copies of e-mail messages may exist, despite end-user deletion, in compliance with Algonquin College's records retention policy. The goals of these backup and archiving procedures are to ensure system reliability, prevent business data loss, meet regulatory and litigation needs, and to provide business intelligence.

Backup copies exist primarily to restore service in case of failure. Archival copies are designed for quick and accurate access by College delegates for a variety of management and legal needs. Both backups and archives are governed by the College's document retention policies. The College policies require that all correspondence with students must be kept for 1 year after graduation of the student.

If Algonquin College discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, e-mail records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify an employee if his or her e-mail records are to be reviewed. Notification may not be possible, however, if the employee cannot be contacted, as in the case of employee absence due to vacation.

Use extreme caution when communicating confidential or sensitive information via e-mail. Keep in mind that all e-mail messages sent outside of Algonquin College become the property of the receiver. A good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "Reply" command during e-mail correspondence to ensure the resulting message is not delivered to unintended recipients.

Access to mail records may occur without the consent of the account owner. The specific policies and process are described in an attached appendix.

Reporting Misuse

Any allegations of misuse should be promptly reported to 5555@algonquincollege.com or by contacting the College ITS Service Desk at extension 5555. If the matter involves confidential information, please contact the Manager of the ITS Infrastructure Services Team directly. If you receive an offensive e-mail, do not forward, delete, or reply to the message. Instead, report it directly to the ITS Service Desk.

Disclaimer

Algonquin College assumes no liability for direct and/or indirect damages arising from the user's use of Algonquin College's e-mail system and services. Users are solely responsible for the content they disseminate. Algonquin College is not responsible for any third-party claim, demand, or damage arising out of the use of Algonquin College's e-mail systems or services.

Failure to Comply

Violations of this policy will be treated like other allegations of wrongdoing at Algonquin College. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use on Algonquin College's e-mail systems and services may include, but are not limited to, one or more of the following:

1. Temporary or permanent revocation of e-mail access;
2. Disciplinary action according to applicable Algonquin College policies;
3. Legal action according to applicable laws and contractual agreements.

Service Definition

Service

The Algonquin College Communications suite encompasses an email, contact and scheduling software environment. This environment is based on the declared supported standards for software at Algonquin College. The current platform is implemented on Exchange 2007.

Client Requirements

In order to access the College's Communications suite, clients must be attached to the College's internal network (either directly or through the College's VPN service) and utilize the standard supported software clients which are:

- Outlook 2007 utilizing Exchange specific protocols. Please note other methods such as IMAP and POP are not supported.
- Outlook Web Access via Internet Explorer 7
- College standard PDA devices

Access to the suite via other methods or clients is not supported.

Email Quota

Each user of the system is provided storage to retain relevant information on the Communications Suite's infrastructure. This information is automatically backed up on a nightly basis by ITS without client intervention. Clients are expected to manage their data within the allocated quota. Currently this quota is set to 1 Gb. Under certain circumstances it may be possible to temporarily increase a client's quota. Requests to increase beyond this level require the consent of the requestor's manager as well as the Manager of the ITS Infrastructure Services Team. Requests should be submitted through the ITS Service Desk. If additional storage is required a service charge may apply. The email system will warn clients when they are approaching the allocated storage limits through the use of an email message. These system messages will be sent when a client's storage reach 80% and 95% warning them that they must clean up their message store to free up additional space. When a client has reached the quota provided it will no longer be possible to send or receive messages until the message store is reduced below the quota.

The message store's deleted messages folder will be emptied each time the client disconnects from the system service. It is important that clients review their deleted messages before exiting the mail client to ensure that there is no loss of data.

Message Sizes

The College restricts the total message size to 10 Mb. Please note that there are other methods available to share larger files with other staff or faculty members, students or external agencies. These include Blackboard, the ITS FTP Service, College Web Site, Committee Minutes Management System and others. Please note when calculating message attachment sizes that the size of the attachment does not always equal the size of a file because of mail encoding methods.

Archive and Storage of Email Database Files (PST files)

The Outlook client provides support for local message stores or PST files. These message stores are not recommended for use by clients for several reasons:

- **Reliability:** These message stores become unreliable and frequently become corrupted once they exceed 1.7 Gb or more than 14,000 messages.
- **Retention:** Local message stores are not backed up by the College's ITS organization. Should the local file system experience a failure these messages will be lost.
- **Efficiency:** The mail system utilizes a single instances message store. This means that a message with attachments is stored only once within the mail system database. By utilizing local messages stores the information is duplicated requiring a greater amount of disk storage to save this information.

A copy of client's communications information stored prior to the migration to the Exchange environment implementation will be made for archival purposes. It is recommended that clients use these files for reference files only and do not actively store new information in these database.

The new Communications suite will limit the use of local PST files through the use of system policies .

Backup and Recovery of Client Data

Backups are undertaken daily in order to secure the production data and to provide for system recovery in the unlikely event of a system failure. Only data that is kept on the central Exchange infrastructure is backed up. Local data files are not backed up. System backups are kept for 6 weeks. Should a Client suffer data loss as a result of a workstation failure or as the result of another fault, requests can be made for the restoration of this data during this 6 week backup "window". Requests for restoration are made through the ITS Service Desk. ITS will make every reasonable effort to restore this information however system users should be aware that these backups are made at a point in time and not continuously. This may result in the information being unavailable for restoration.

Mass Mailings

ITS maintains mailing list systems with a series of predefined group of mailing or distribution lists to provide methods to communicate with all the staff or the College or subsets of clients. Access to these mailing lists is restricted to ensure the system is not abused. Permission to utilize these mailing lists are managed through an ITS Service Desk request which must be approved by the College's CIO.

Other mass mailings can be set up for external or internal distribution lists which will be maintained by the requestor. Requests for these mailing lists are made through the ITS Service Desk and must be approved by the Manager of the Infrastructure Services Team.

Application or System Mail Integration

Upon request and with the approval of the College's CIO, systems and applications will be allowed to send or receive mail through the College's mail infrastructure. These requests are made through the ITS Service Desk. All other mail traffic will be blocked by the College's network infrastructure and firewalls.

Email Alias

Each mail account will have an email alias provided which is based on the clients first name and last name. In cases of a conflict with an existing mail account, ITS will provide an alternative address which is similar to this.

Common Directory

Each mail account will have an entry in a common directory which will be addressed as the global directory. Clients are encouraged to use this directory to determine mailing addresses rather than guessing another user's mail account.

Generic or Group Email Accounts

Information Technology Services discourages the use of generic or group email accounts for a number of reasons including security and management. However there are times when it is necessary to publish an address that is related to a service or program. Clients are strongly encouraged to utilize an email alias which can be used to mask an individual email account or to forward messages on to a group of users. Requests for these services must be reviewed and approved by the Manager of the Infrastructure Services Team. Requests for these services are made by through the ITS Service Desk.

Unsolicited Email and Virus Scanning

Information Technology Service under takes a number of processes to minimize the possibility that messages that are sent or received contain viruses, unsolicited commercial email, or phishing scams. As with any set of automated tools it is impossible to complete eliminate all unwanted messages. It is also possible to lose legitimate email messages that were incorrectly

classified. If you are concerned about the messages you are receiving (or that are being blocked) please contact the ITS Service Desk,

The College Communications suite utilizes several independent layers to provide integrated spam filtering and the junk mail filtering. The first layer isolates the College email system from the Internet through the use of CanIt Pro. This system filters out specific file types, detected viruses as well as performing analysis of messages to reduce the numbers of unsolicited commercial email. All messages leaving, entering or transiting the College e-mail system will pass through this filtering before delivery. Many of the options for this service are user configurable. For information on this system please contact the ITS Service Desk. Additionally the Microsoft Exchange environment utilizes the Forefront message hygiene system which scans messages through the use of several independent virus and unsolicited commercial email scanning tools.

Client Configuration Options

The Outlook mail client contains tools that allow clients the capability to white list or black list specific mail senders. It also includes heuristics to scan for unwanted commercial email. Clients are cautioned that the configuration and use of this tool may lead to lost messages which will be unrecoverable by Information Technology Services. Please note these tools only function when the messages are received through the Outlook mail client and do not apply when the Outlook Web Access Client is utilized to access mail.

Bulk Mail Labelling

The College's automated filters will label all suspected email that may be unsolicited commercial email by placing a [Bulk] tag in the messages subject line. It is recommended that these messages be filtered to the Client's junk mail folder for occasional review and management.

Blocked file types

The College's Communications Suite automatically blocks several file types based on industry based best practices to limit the College's exposure to malware. The file type filtering is based on the three letter suffix of the file name. Clients should always exercise caution when opening attachments received by email even with these measures in effect. These file types are:

File Type	
.EXE	Executable files
.PIF	Windows Command Script
.BAT	Windows command script

User Training

All new users shall be given appropriate basic training in the use of the ITS Communications Suite. ITS provides several excellent computer based training (CBT) courses which allow self study in the use of the software components that make up this suite. Links to these courses are

maintained on the ITS website at <http://www.algonquincollege.com>. Additional, advanced or retraining courses can be arranged on request through the ITS Service Desk.

Service Level Expectations

System Hours

The College's Communications suite will be available 24 hours a day 7 days a week. Exceptions to this service availability will be unplanned outages as the result of a system failure or planned maintenance. Planned maintenance will be minimized as documented in the System Maintenance Directive.

System Availability

The expected service uptime is 99.9% with a 30 minute recovery time should a system failure occur. It is expected that all client data will be maintained in the unlikely event of a catastrophic system failure. The recovery time for a catastrophic failure is expected to be 1 working day.

Service Performance

This Service Level Agreement does not define the response times which will be achieved. However the significance of appropriate response times is recognized. Where there are specific problems in this area, please reports these issues to the ITS Service Desk. These requests will be reviewed by the Infrastructure Services Team who will take the appropriate action.

Service Maintenance

The College's Communications Suite will be maintained as per the guidelines laid out in Directive A23 Information Technology Scheduled System Maintenance.

Scheduled System Maintenance

The College Communications Suite requires 4 hours per month maintenance, during which time the system is unavailable. This maintenance will take occur between 04:00 AM and 08:00 AM on the first Sunday of each month.

Incident Management

The Service Desk is available to all users and is the first point of contact for any problems or queries. The Service Desk provides assistance with all aspects of the ITS services either directly or via specialists.

SERVICE DESK TELEPHONE NUMBER IS: x 5555 or via email at 5555@algonquincollege.com

The Service Desk operates from 7:30 AM to 10:00 PM 7 days a week. The service is available all year with the following exceptions:

- Between Christmas and New Year's Day

After hours reporting of incidents is provided through voicemail and email.

Change Management

Any changes to these services will be managed through the documented ITS Change Management process. This process has been established to optimize the rate of change while containing the risk of adverse impact on service levels.

Service Level Monitoring

ITS monitors and reports upon the levels of service delivered and compare these to these documented service levels. Where a failure to meet requirements has occurred, the necessary action to prevent a reoccurrence will be initiated.

Service Performance Reporting

Service Performance Reporting will be performed on an ongoing basis.

Policies Related to Non-Consensual Access to Email

Access to mail records may occur without the consent of the account owner. The specific policies and process are described in an attached appendix. The College shall only permit inspection, monitoring or disclosure of email when:

- 1) When required by and consistent with law enforcement and the law
- 2) When there is a substantiated reason to believe that there has been that governing policies or laws have been violated as spelled out in these terms of use.
- 3) When there is a compelling situation or situation that necessitates this access;
- 4) Or, under time-dependant, critical operational circumstances.

Except in these emergency circumstances such actions will be authorized in advance by the appropriate College party. Where required this access will be limited to the minimal perusal of content or action to resolve the situation.

Request for access to email accounts must be authorized by the appropriate College party via a formal written document in the format provided. The appropriate College party is:

Email Account Holder	Authorizing Official
Faculty	Academic Chair, Executive VP Academic after consulting with the HR Department
Staff	Executive VP after consulting with the HR Department
Administrative Staff	Appropriate Executive VP after consulting with the HR Department
All Staff or Faculty	Health and Security Services after consulting with the HR Department

This authority may be also provided by the President of Algonquin College or the Vice President of Human Resources without regard to the email account holder. This authority may also be further delegated.

Authorization for Non-Consensual Access to Email Records

This form should be completed when requesting access to a users communications records when consent has not been received. ITS must receive a completed authorized before access is provided.

Date: _____

Employee name: _____
Last *First* *M.I.*

Job title: _____

Supervisor: _____ Department: _____

Description of Access Required:

Additional comments:

Approval

Date

Table of Contents

Table of Contents

Faculty and Staff Communications Suite Terms of Use.....	1
Scope	1
Account Activation/Termination	1
General Expectations of End Users	1
Appropriate Use.....	2
Inappropriate Use	2
Monitoring and Confidentiality	3
Reporting Misuse.....	4
Disclaimer	4
Failure to Comply.....	4
Service Definition.....	5
Service	5
Client Requirements	5
Email Quota.....	5
Message Sizes.....	6
Archive and Storage of Email Database Files (PST files)	6
Backup and Recovery of Client Data	6
Mass Mailings	7
Application or System Mail Integration	7
Email Alias	7
Common Directory	7

Generic or Group Email Accounts 7

Unsolicited Email and Virus Scanning 7

 Client Configuration Options 8

 Bulk Mail Labelling 8

 Blocked file types 8

 User Training 8

Service Level Expectations 9

 System Hours 9

 System Availability 9

 Service Performance 9

 Service Maintenance 9

 Incident Management 9

 Change Management 10

 Service Level Monitoring 10

 Service Performance Reporting 10

Policies Related to Non-Consensual Access to Email 11

Authorization for Non-Consensual Access to Email Records 12

Table of Contents 13

Change Management Log 14

Change Management Log

Please ensure the change log is maintained by updating this table each time the document contacts are revised.

Draft	2008-10-24	Initial Draft	Rod Martin
Version 0.1	2008-11-09	Incorporated feed back related to message archiving and quota.	Rod Martin
Version 0.2	2008-12-11	Incorporated comments	Rod Martin
