Q2 2025-2026
Email Best Practices

We hope you all had an excellent Fall Term ACDay1 and are looking forward to an exciting year ahead! Fresh starts always come with a lot of new information and documents that need to be shared, which at times will involve personal information (PI). This is a great opportunity to go over some best practices when it comes to one of the most common ways we circulate data, and a frequent way breaches occur – email. Here are 5 tips to keep your inbox breach free and compliant with policy IT01 Information Security:

1. **Do not send unprotected attachments containing sensitive PI.** Instead, we recommend using SharePoint links with specific permissions applied so only those authorized can open the document, which should also be password protected. The password should be shared in another format with the intended recipient. If your email is sent to the wrong address, these methods make it much easier to limit the exposure of PI to unauthorized individuals. Misdirected emails are a frequent cause behind privacy breaches, as observed by our own Privacy Office as well as the Office of the Information and Privacy Commissioner of Ontario.
2. **Algonquin-issued emails must be used when conducting College business.** This practice must always be followed whether you are an employee writing to a student, or to another employee. This ensures appropriate safeguards are in place to protect incoming and outgoing content. Refrain from using personal emails as there is no way of verifying whether content sent to an external email address is secure, or accessible to only the person you intended. Additionally, emails sent to external addresses cannot be recalled, making it impossible to retrieve misdirected mail. Please refer to s.2.7 in policy IT01 where this requirement is set out for employees, contractors, and learners.
3. **Verify your recipients, especially when sending to a new or infrequent recipient.** Outlook has a handy feature where it will autofill emails based on the letters you type. While this can be a great time-saving feature, it can result in the wrong address being populated. Take a moment to double-check that your recipients are correct before hitting send. A few extra seconds of caution can prevent a serious and costly breach.
4. **Ensure recipient fields are used appropriately.** If you are writing to a group of learners, the BCC function should always be used as the CC and TO fields leave emails visible to all recipients. If you are communicating with external parties, consider whether BCC is more appropriate in your circumstances.
5. **Be cautious with forwarding emails.** Lengthy email chains can sometimes be a minefield of risk when it comes to sensitive PI. Before forwarding or replying in a chain, ensure that all recipients are authorized to view the content being discussed, including any attachments or links.

Thank you for taking the time to learn a bit more about how to keep your email breach-proof!

If you ever have any privacy-related questions, or if you'd like to suggest a future newsletter topic, please reach out to the Privacy Office using the email below, we'd love to hear from you.

And remember, Information Security and Privacy is everybody's business!

PRIVACY QUESTIONS?
EMAIL PRIVACY@ALGONQUINCOLLEGE.COM