Welcome to Day 3 of Data Privacy Week as we explore information handling best practices so you can protect data at every step in its life cycle. Yesterday we discussed identity verification, consent and authorizations, and consistent use. Today we'll be tackling the practice of "need to know", as well as sharing and transmission. These practices directly contribute to proactive risk mitigation, helping us protect personal information (PI) the College holds against real and probable threats.

Need to Know
The concept of "need to know", also known as the "principle of least privilege", requires that employees be given only the minimum level of access rights and permissions needed to carry out their role and any related responsibilities. This includes having a process in place to ensure employee permissions are regularly reviewed to assess if any operational or personnel changes have occurred that should impact the level of individual access.

In the event of a breach or account/system compromise, this practice helps to reduce the potential scope of damage and loss to individuals and the College. For example, when properly implemented, limited permissions can help stop the spread of malware, or limit an attacker's ability to gain access to more sensitive information or systems. When faced with strict permissions that do not allow for deeper incursion, the risks these attacks pose can be reduced or eliminated entirely.

Sharing & Transmission
Whenever PI needs to be shared or sent, it's imperative that before you complete the action, you take a few moments to double-check that everything is correct. With respect to emails, this can look like verifying the addresses of anyone who will be receiving the information, and ensuring attachments are correct and do not contain any extraneous information. Also consider whenever possible using links rather than attachments to allow for more reliable permissions management, especially in the event of an error. For a deeper dive into email best practices, please review the Privacy Office's Q2 Privacy Beacon newsletter which was sent to all employees on September 29th.

In terms of sharing information through a platform like Sharepoint, precautions should involve reviewing individual permissions so they are limited to only those who need access for their role, removing permissions in a timely manner after the information has served its purpose, and password protecting documents containing PI.

Thank you for spending time with us while we share as valuable guidance on how to keep data safe and secure. Tomorrow we'll be exploring the last three principles, so be sure to keep an eye on your inbox.

In the meantime, if you have privacy questions or concerns, you can reach out to the Privacy Office any time at privacy@algonquincollege.com with your queries. You can also visit us today at the Data Privacy Week Information Booth from 12PM to 2:30PM in the Marketplace Food Court, where the Privacy Office will be available to answer all of your privacy-related questions. Be sure to stick around for games, swag, and more!

Staying informed about privacy can help you stay proactive in your efforts to keep personal information safe and secure. And remember, Information Security and Privacy is everybody's business!

PRIVACY QUESTIONS?
EMAIL PRIVACY@ALGONQUINCOLLEGE