**TIPS ON DEVELOPING A PRIVACY CULTURE.**

Data privacy is simply about your right to protect your personal information. Personal information is any information that can be used to identify an individual. Data privacy does not equate to secrecy; it is the individuals’ right to know how organizations collect, use, store, and disclose their personal information.

As Algonquin College is an organization that processes a high volume of personal information, it is essential to imbibe a culture of privacy beyond a check box exercise. An environment that is “privacy culture-centric” will help build a strong foundation of customer trust that can be used as a competitive advantage. The biggest threat to developing this culture is the people, so each employee must recognize and value their role in building a culture of privacy at the College.

Please see below some tips for helping to build a privacy culture at the College:

* **Privacy by design and default**: For products, services, processes, and solutions that will involve the processing of personal information, ensure that privacy is considered and built-in at the initial design stage and throughout the development cycle and not as an afterthought. Ensure that you collect the minimum personal information necessary for a specific purpose when you need it and use it only for that particular purpose. For secondary purposes other than personal information collected, ensure you seek and receive informed consent from the individual except if the secondary purpose is permitted by law or consistent with the original purpose. Contact privacy@lgonquincollege.com for more information.
* **Data breach incidence**: Do not attempt to handle data breaches alone. Once there is an incident, promptly report it to privacy@algonquincollege.com (even if unsure). **This is mandatory.**
* **Email**: Do not share sensitive information (i.e., a document that contains personal health information) in an email as emails sent over the internet are not secure and may be lost, misdirected, intercepted, misused, or altered if you must do so; ensure to secure the document with a password, and share this password via another channel (i.e., Teams). The best practice is to share the private link to the document with the specific recipient.
* Take a minute to verify the recipient’s email address before sending. If sending a confidential email to a large recipient, ensure you send it using BCC.
* **Limit access on a need-to-know basis**. Only give access to records containing personal information to colleagues who need it to perform their jobs. The fewer people who have access, the fewer risks there are for privacy breaches.
* **Maintain oversight of vendors.** Did you know that when you procure third-party services, the College remains fully accountable for how they access, collect, use and protect the privacy of the personal information you entrust to them? Did you know that third parties doing business with the College generally do not accept any responsibility for privacy breaches, including breaches caused by their negligence? Not to worry. The College has established a process to assess the reliability of third-party vendors. It has developed contract clauses to ensure that third parties handle personal information in a way that enables the College to comply with applicable legislation. Before procuring third-party services with access to personal information, contact the ITS Business Relationship Managers (BRMs)to determine the initial steps required
* **Zoom and Teams meeting:** Ensure you have a real and necessary purpose for recording meetings. Ensure all attendees know you will be recording the session when sending the invite. Do not use these services to share sensitive or confidential files.
* **Teams/SharePoint:** When creating a Team/SharePoint site, ensure it is set up as private and not public. When sharing a document on these sites, ensure to share the link to “*specific people*” and not “*people in Algonquin College with the link*.” This way, you will prevent unauthorized people from accessing the document, even if the link was inadvertently shared with them.
* Familiarize yourself with our [**IT01 Policy**](https://www.algonquincollege.com/policies/files/2021/01/IT01.pdf) to know more about your responsibilities in protecting College information and technology. For all employees, ensure to complete the [**Online Information Security and Awareness Training**](https://employeelearningcatalogue.algonquincollege.com/course/344/information-security-awareness-and-training) to learn how to keep sensitive and valuable College information, including that of our learners and employees, safe.

For more information or inquiries, please get in touch with privacy@algonquincollege.com.

**Information security and privacy are everybody’s business**.