Welcome to Day 2 of Data Privacy Week! Over the next three days, we'll be exploring eight information handling best practices, beginning today with the first three: identity verification, consent and authorizations, and consistent use.

Guided by legislated requirements, these three principles work in tandem to establish a solid foundation upon which all future interactions with the individual and their personal information (PI) will be built. In the absence of any of these elements, the College cannot proceed with actions such as collection or use of PI.

Identity Verification

This is the first and most important consideration in responsible information handling because you can't do anything without it! Before taking any action involving someone's PI, you must first confirm you are dealing with the individual who owns the PI, or someone they've authorized to act on their behalf.

Identity verification can be carried out by several means, including asking a series of questions only the individual would know, or requiring the person to produce an identification document like a driver's license or student card. And always be wary of malicious actors! Social engineering tactics are common tools used to commit identity fraud, and with the introduction of generative AI, these threats are now heightened. AI can be used to mimic someone's writing style, or even their voice over the phone or via video (Deepfakes) making it harder to spot a threat.

Consent & Authorizations

Once you've confirmed you're speaking to the right person, the next key step is to ensure you have up-to-date consent to carry out the requested activity with their PI, such as collecting or modifying it. Individuals may also authorize someone else to act on their behalf, like a parent or spouse. In scenarios such as this, no actions should be taken beyond what the data owner has authorized. For example the data owner may have consented to their PI being disclosed to the authorized individual, but did not consent to them being able to modify or delete their information. There may also be a limitation or an expiry on the authorization, so always be sure you are relying on current direction from the individual.

Consistent Use

When first obtaining consent, the individual must be told why their PI needs to be collected, the purpose it will be used for, whether it will be shared with anyone, and how long it will be kept before being securely disposed of. This should be done with a privacy notice at the time of collection. The College is only allowed to use PI for the purpose it was collected, or for a purpose consistent with the original reason. If there is any change in purpose, or expansion of purpose that goes beyond the original reason for collection, a new consent/authorization will be required.

Thank you for taking the time to learn about these important principles. We'll have more for you tomorrow so stay tuned!

In the meantime, do you have privacy questions or concerns? Reach out to the Privacy Office any time at privacy@algonquincollege.com with your queries. 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!