

Privacy Best Practices

Privacy Protection is everyone's responsibility. Below are some tips to help you meet privacy requirements.



1. Double-check email addresses and make sure you have the correct attachment before clicking send. Incorrect addresses and documents are the leading cause of privacy breaches.



2. Never share usernames, passwords, access codes, or other credentials. You are responsible for all activity under your user credentials and your activity can be audited.

3. New projects or initiatives involving personal information require a [Privacy Impact Assessment](#).



4. Only use personal information for your role, and use the minimum amount needed for the task.



5. Do not keep personal information longer than you need to. Securely dispose of records and information no longer required in accordance with TMU's [Records Retention Schedule](#).

6. Concerned about a potential or actual privacy breach (including through loss or theft)? Immediately contact the Privacy Office using the [Privacy Incident Reporting Form](#).



7. For more information about privacy requirements and best practices, review TMU's [Privacy and Access-to-Information Policy](#) or contact the Privacy Office at privacy@torontomu.ca.

