Best Practices for Protecting Personal Information When Using Email

- Include a notice in email messages that the information contained is confidential—include instructions for response if email is received in error. This notice can be sent automatically by including it in your signature. To create a signature in Outlook open an outgoing message, click on **Signatures** (banner along top) and create your signature OR click on **File**, then **Options**, then **Mail**, then **Signatures**. Feel free to use the following example:

  PLEASE NOTE: The information contained in this email message and any attachments is privileged and confidential, and is intended only for the use of the recipient(s) named above. If you have received this email in error, please notify me immediately and delete this email and any attachments without copying, distributing or disclosing their contents. Thank you.

- Always use your Trent email account for sending work-related messages.

- Confirm that the email address you are sending the message to is current.

- Periodically confirm recipients and email addresses for all distribution lists.

- Instructors should use class lists provided through the Office of the Registrar; student emails should not be requested by passing a blank piece of paper around the class.

Device Security

Information you receive and send in email is stored on devices that you have connected your email account to – phones, tablets, laptops and desktops. Any devices where you check your email could have traces of personal information you've received or sent.

- Make sure devices, especially mobile devices, are encrypted and protected with a high quality password. For more information on encryption - https://www.trentu.ca/it/services/encryption.

- Take appropriate physical security measures to protect devices
  - Do not leave devices in plain sight when traveling.
  - Do not leave mobile devices unattended.
  - Always store larger mobile devices (tablets and laptops) in the trunk or storage area of a vehicle when traveling.

- Never store personal information on a USB stick or non-university file storage application (Dropbox, Google Drive, personal OneDrive).

- Avoid using shared devices (kiosk computers, hotel computers) to access Trent email or any personal information stored on Trent systems.

Other security measures

- Password protection should be used when creating any documents containing confidential information. Do not send the password in the same message as the attachment.

- Double check emails to confirm attachments are correct and should be there.

Office of Provost & Vice President Academic
October 26, 2016