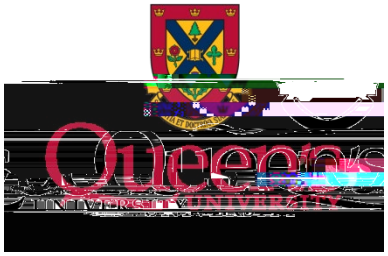

PRIVACY BREACH PROTOCOL

If a privacy breach occurs, take immediate action

Maintaining privacy and confidentiality

Queen's University is subject to various regulatory and policy-driven requirements regarding privacy and confidentiality of information, including the Freedom of Information and Protection of Privacy Act (FIPPA), the Personal Health Information Protection Act (PHIPA), the Electronic Information Security Policy Framework, and the Records Management Policy. These requirements must continue to be met by Queen's employees who are working remotely.

Remote workers are required take all reasonable steps to secure and maintain the confidentiality of Queen's University information and records while they are being transported to and from an employee's off-site workspace, and while the documents are stored at the off-site workspace no matter if the information is in physical or digital format. Records and information must be protected from being damaged, destroyed, stolen, copied, or otherwise accessed by unauthorized individuals.

- When remotely accessing records and information it is essential that employees use the Queen's Campus Virtual Private Network (VPN). The Queen's VPN (Fortinet FortiClient) is a safe and easy way to ensure a secure, remote internet connection to on-campus resources.

- Any device (such as a laptop, desktop, cellphone) used to perform university business must be encrypted. This includes personal devices such as a personal cellphone or home computer. Encryption protects against a data breach even if the device is lost or stolen. Ensure that "Find my Device" is enabled or that the "Find My" app is installed so that in the event of a theft, the device can be located, locked, or erased remotely.

- Queen's employees working remotely must not allow anyone else, such as a spouse or child, to use devices that contain work-related documents. In addition to being encrypted, devices must be password protected and those passwords are not to be shared with others, including family members. Screens should be set to lock when not in use. Employees should also be conscious of the visibility of their screen to other people in the remote workspace when accessing confidential university records and information.

-

- The language and conduct of the chat should always be professional. Additionally, these messages may need to be preserved if they contain substantial decisions or other university business.

- If messages are transitory and are deleted after they have been read there is still often evidence of this deletion

Helpful resources

- Data Security and Encryption: Handling Confidential & Personal Information
- Protect Your Virtual Meetings , Queen's Gazette, 4 February 2021
- Connecting, Collaborating, and Teaching Remotely
- ITS Information Security
- Records Management and Privacy Office