Fact Sheet

Working Remotely: Access to Information, Protection of Privacy, and Records Management

Records Management and Privacy Office
Kingston, ON K7L 3N6
Tel. (613) 533-6095
access.privacy@queensu.ca

Now more than ever before, large numbers of Queen's employees are working remotely. Some may find difficulty in completing tasks they used to do with ease in the past, in part due to new and different work environments. The shift to a remote environment may necessitate using non-university resources such as private internet connections, personal telephones, and home computers.

The ability of the Queen's community to adjust to this new work reality is laudable and shows employees' adaptability, resourcefulness, and commitment. What may not be top of mind is employees' continued recordkeeping responsibilities, ensuring that records documenting university decisions and actions are created and retained, and that information is properly managed at all times. Good recordkeeping is accomplished by being forward-thinking and by using the correct tools in an appropriate manner.

In accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA), Queen's has a continued obligation of transparency and accountability to the Queen's community and the general public who all have a fundamental right to access the university's general records and their own personal information.

Employees must ensure they take adequate measures to preserve the university's records and information by working conscientiously and following the practices below.

Avoiding a privacy breach

The change in work routines not only raises concerns about maintaining employee effectiveness and productivity, but also risks the potential of a privacy breach if physical and digital environments at home are not as secure as the ones provided to employees at their office. Queen's University employees handle a wide array of personal, health, and other confidential information, and must do their utmost to ensure that their remote work environments offer the same level of protection as their work environments on campus.

If a breach of privacy occurs or is suspected, read and follow the privacy breach protocol and contact the Chief Privacy Officer as soon as possible.

PRIVACY BREACH PROTOCOL

If a privacy breach occurs, take immediate action

CONTAIN: stop or contain the breach if you can

REPORT:

- to your immediate supervisor (or, if unavailable, the next level of management) and the unit or department head
- to the Chief Privacy Officer at access.privacy@queensu.ca or (613)533-6000 ext. 75226 who will assist with the next steps

INVESTIGATE: use the step-by-step **Privacy Breach Report Form** (to be provided by the Chief Privacy Officer) to collect information and address the breach

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.

- With respect to hardcopy documents, employees must be careful about who can view them during the day, and store them away in a box or file folder when not in use. At the end of the day, lock them away in a cabinet or closet if possible.

- When destroying transitory records, employees must take measures appropriate to the medium. Digital records may simply be deleted, while non-confidential hardcopy records may be recycled. Ensure that confidential hardcopy documents are shredded using a cross-cut shredder. If such a shredder is not available in the remote workplace, return confidential documents to campus for appropriate disposal using university vendors or facilities. Review the Data Classification Standard to ensure documents you are intending to dispose of are destroyed appropriately.

- For disposal of official records, ensure they are eligible for disposal by referring to the Queen's University records retention schedules or contact the Records Manager for assistance.

Teleconferencing and video conferencing

When taking part in a teleconference or video conference, employees should maintain an awareness of the confidentiality of those meetings, classes, or events. Consider whether it is possible for others in the remote workplace to overhear confidential conversations. Whether you are the host or a participant, take note of these tips for enhancing confidentiality.

- Be mindful that while many devices have video capability, some individuals may prefer to participate using voice only, or to obscure the background of their meeting space.

- Unless there is a compelling reason to do so, avoid taking screenshots or video or audio recordings of meetings, classes, or events. Such images and recordings become records and require proper management and storage. Furthermore, they may become subject to an access to information request.

For information about confidentiality and privacy in the remote classroom, see the fact sheet on **Privacy and Remote Teaching & Learning**.

- If recording or taking a screenshot is desirable, give participants notice in advance. Some tools such as Microsoft Teams automatically notify participants when a meeting is being recorded. The notice should also be repeated at the beginning of the recording to document the notice and to state the purpose of the recording by the person who intends to record.

- If a recording is made, it should be retained no longer than necessary and deleted after its purpose has been met (e.g., after meeting minutes have been created). Recordings leave a variety of indicators as to their creation, existence, and, depending upon the technology used, even their deletion.

If teleconferencing or video conferencing is used to facilitate student advising or other kinds of medical or counselling activities, it is **essential** that privacy is maintained. **Employees must ensure their work environment is private**, and that the use of any recording technology will be done only with consent. **Consent must be documented**. Furthermore, only secure platforms may be used. See the resources listed below and seek guidance from IT Services if you are unsure about which platform to use.

Creating and managing university records

As university employees work remotely, more university business is being handled using a variety of technologies that document our efforts, including email, chat logs, text messaging, and virtual meetings. While some records may be created with intent, some tools create ancillary records, leaving "digital tracks" of the work employees do. While some of these tracks are useful, others are transitory fragments that add up to very little. When using online tools, employees must realize that their text conversations, recordings, and even sharing of files could become matters of public record.

- **Chat messages** in the Posts tab of a Teams space, or as a message in a Teams or Zoom meeting, are no different than email messages in that they are in fact records. While messaging is often less formal and more fluid than email, the messages, when they relate to university business, **are university records**.

- 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, so be mindful of what is put into a chat and be aware that the deletion itself is visible and can look questionable even if the content was benign.

- In some instances, it may be desirable to connect with your colleagues via a phone call or a video meeting rather than use messaging functions especially when dealing with the personal information of students.

- Be mindful that some of what is communicated using these various tools may need to be produced as evidence of decisions or actions taken, or to satisfy legal inquiries or access to information requests.

FIPPA applies to records in the custody or under the control of an institution. Emails, chats, texts, and other communication sent or received for business purposes, even those sent using personal accounts, have been found by Ontario's Information and Privacy Commissioner to be under an institution's control for the purposes of FIPPA and therefore required to be disclosed. Accordingly, always use these tools mindfully.

When employees return to campus after a period of remote work it is crucial that the documents they removed from their office be returned and that any records created while working remotely are filed in their unit's recordkeeping systems, both hardcopy and digital.

Access to information rights

Employees must be mindful that Queen's University has a legal obligation to provide access to information and ensure reasonable measures are in place to document and preserve records, and that this obligation continues to apply to all employees who are working remotely.

- All work-related records continue to be subject to access to information legislation, regardless of whether they are retained on Queen's-issued or personal computing and storage devices.

- Employees should continue to use established records management practices and file records in Queen's recordkeeping systems.

- When working remotely employees must digitize or transfer all business records to work-related systems and repositories as soon as possible to allow for improved access controls and security to be applied to the records.

- Employees must appropriately back up business records when using personal computing and storage devices if files are not retained in Queen's IT Services-supported storage spaces such as the departmental shared drive or an MS 365 cloud tool like SharePoint.

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