BRANDON UNIVERSITY

Online teaching technologies: privacy and security overview

Recording

- You must obtain consent of a presenter (e.g. guest lecturer) before recording the lecture.
- You must obtain consent of a presenter (e.g. guest lecturer) before posting a recording of them to a course website or any other website.
- You must inform the audience that a lecture is being recorded for purposes of a course.
- You must obtain consent from participants if posting a lecture, discussion, or portions thereof (e.g. screenshots) to a website or social media platform separate of the course itself.
- Audience members may choose to turn off video when lectures are being recorded.

Personal Information

- Personal information about course participants (e.g. accommodations, course performance) must not be shared or recorded in a way to make that information visible to other participants.

Line of Sight/Sound

- You must be mindful of who might be in the background of a video, or within range of hearing your conversation.
- Close applications that may contain private or sensitive information (e.g. email or class lists) prior to sharing your screen with a group.
- Take care in discussing information that could be personal in nature on collaborative applications.
- Maintain a respectful tone in your communications online – written, visual, and verbal. Communicate in ways which respect the spirit of the Student Non-Academic Misconduct Policy and the Brandon University Discrimination and Harassment Prevention Policy.

Audit Capabilities

- You must inform the class cohort if you are using system audit capabilities to evaluate course performance (for example, tracking completion of required readings as noted in system logs).
- Chat thread records are retained on backend servers. As with email, chat threads are subject to information request under FIPPA. Please take care in discussing sensitive or personal information in chat threads and maintain a respectful tone.

Security Reminders:

- IT Services will never send you an unsolicited email or message asking you to click a link or ask for your password. Reputable companies and institutions will never ask you for your password.
- Do not click on any links or open any attachments you received in an email or other message unless you have verified the sender.
- If you have received a suspicious message from someone you know do not reply to it. Contact the person by other means to confirm.
- If you are unsure if an email is legitimate send it to antispam@brandonu.ca
- Use different passwords for all your online services.
    - For example, your online banking password should be different from your Facebook password.
- Use easy to remember password phrases longer than 12 characters.
    - For example: My1Dog*Ate*My$Homework!
- Consider enrolling in the multi-factor authentication tool, which will push validation codes to your smartphone, and allow you to keep the same password for a one-year period. Email helpdesk@brandonu.ca to enroll.
- For more detail please visit Brandon University's IT Security Website.