No.949113

ACCESS & PRIVACY BASICS FOR NEW STAFF

The St. James-Assiniboia School Division follows the *Freedom of Information and Protection of Privacy Act* (FIPPA) which:

- Protects privacy by regulating how personal information is handled
- Provides for public access to information through formal requests for Division-held records

What Does This Mean?

- Personal information is information about an identifiable individual
- Privacy protection is common sense
- Protect personal information from unauthorized access or loss while using it for Divisional purposes
- Privacy protection is a shared responsibility requiring your participation
- Everyone who works at the Division is responsibl`e for protecting personal information
- Everyone should identify, report and help remedy privacy issues at the Division

Key Things to Note:

Think before you "say" it – would you be prepared to have your response published in the newspaper – maybe even the front page?

When you respond to / email / speak to a member of the public (parent, community resident, etc.) keep in mind everything is "FIPPA-able", meaning that it can be requested and potentially accessed by that person. There are exceptions that protect certain types of information as well as the rights of others.

What is a "Record"?

- **A** "**Record**" or "**recorded information**" means a record of information in **any** form, and includes information that is written, photographed, recorded or stored in any manner, on any storage medium or by any means, including by graphic, electronic or mechanical means. This includes:
  - Emails from your Divisional email address
  - Text messages sent from Divisional devices
  - Recorded conversations – verbal recordings or written notes from a conversation

Please Ask! - If in doubt, please ask your access and privacy questions of:

- The Division's Access & Privacy Coordinators (extension 2010 or 2009)
- Address privacy issues **when they arise** with your supervisor and/or the Access and Privacy Coordinator

Other Tips:

- Lock your computer screen when not at your desk
- Do not have your password written down and displayed on your desk / computer screen
- Keep confidential work "face-down" when another employee approaches your work area
- Only collect personal information that you need to do your job
- Encrypt electronic personal information that is not in a secure Division server
- Keep hard copy personal information locked and away from the public
- Avoid inadvertent exposure of personal information at work, home, transit and elsewhere
- Deposit confidential shredding in the shredding consoles at your office / school
- Destroy personal information securely – cross-cut shred and ask IT staff to destroy electronic records
- Immediately notify the Access & Privacy Coordinators of any potential breaches so you can work together to come to a solution

For more information, please review the following:
https://www.ombudsman.mb.ca/info/fippa.html