Strait
Regional Centre for Education

Privacy 101: Tips and Best Practices

As employees of a public body, and in accordance with the Freedom of Information and Protection of Privacy (FOIPOP) Act, we all have a responsibility to keep student and staff personal identifying and sensitive information secure and confidential. Further, we are required to protect the personal information in our care by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. By doing so, we are fulfilling our obligation to protect an individual's personal information and preventing a privacy breach.

What is Personal Information?

Personal information is recorded information about an identifiable individual, including:

- the individual's name, address or telephone number;
- the individual's race, national or ethnic origin;
- colour, or religious or political beliefs or associations;
- the individual's age, sex, sexual orientation;
- marital status or family status;
- an identifying number, symbol or other particular assigned to the individual;
- the individual's fingerprints, blood type or inheritable characteristics;
- information about the individual's health-care history, including a physical or mental disability;
- information about the individual's educational, financial, criminal or employment history; and
- anyone else's opinions about the individual, except if they are about someone else.

Source: FOIPOP Act, Section 3(1)(i)

Emails and Facsimile

- Use the 'bcc' field when sending an email to multiple personal addresses.
- Be mindful of 'auto name completion' to ensure you are sending to the right recipient.
- Before emailing sensitive information, ensure that either the owner of the sensitive information has consented to the transmission via email, that the information is encrypted or sent via secure FTP sites.
- Always include a confidentiality clause and signature block.
- Do not use personal quotes on the bottom of emails. Unrelated content has no place in a professional email.
- Before faxing sensitive information, ensure that you are sending to a secure fax machine. Prior to sending a fax, call the receiver to confirm that the receiving fax machine is secure and to confirm the fax number. Always use a cover sheet that includes both the sender's name and telephone number and the intended recipient's name and phone number. Always attach a confidentiality notice.

Strait
Regional Centre for Education

Privacy 101: Tips and Best Practices

Technical Security of Electronic Files

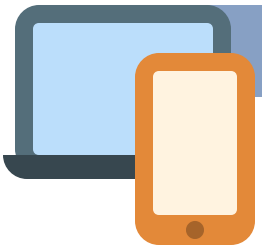
- Create a strong, complex and unique password comprised of a minimum of eight (8) characters, preferably more. Three of the following four character sets must be used: uppercase letters; lowercase letters; numbers; and special characters (e.g., @ / # / ! / $ / + / =). Avoid common or obvious passwords (e.g., dictionary words).
- Never auto-save passwords for sites that contain sensitive information (e.g., PowerSchool, webmail).
- Use different passwords for different sites and do not use home passwords at work.
- All electronic files containing sensitive information must be stored on a secure central server, not on a local hard drive.
- Encrypt highly sensitive confidential personal information.
- Do not post your passwords on your desktop or anywhere else they may be viewed.
- Ensure information on network drives is only accessible to those who need it.
- Position computer screens so they are not easily visible to others.

Physical Security

- Store files/devices containing personal information in a locked filing cabinet and never in your vehicle.
- Only remove documents from your office/classroom if they are necessary to carry out your duties, and only remove the absolute minimum you require.
- Clear your desk of all files with personal student/staff identifying and/or sensitive information.
- Lock your office/classroom door when you leave.
- At the end of the day, log off all systems.
- Do not open or review confidential information if it can be viewed by others.
- Ensure documents are not left in meeting rooms, on flip charts or written on white boards.
- Remove documents from photocopiers, faxes and printers as soon as possible or use the secure print function if available.
- Dispose of hard copy records containing personal and sensitive information by placing them in a secure (locked) shredding bin or by shredding them yourself.

Strait
Regional Centre for Education

Privacy 101: Tips and Best Practices



Mobile and Portable Devices

- All mobile and portable devices shall be password protected.
- Store mobile and portable storage devices such as laptops in a locked cabinet and never in your vehicle.
- Ensure all personal and sensitive information on a portable storage device is limited to the absolute minimum necessary and is encrypted.
- Permanently delete personal and sensitive information on a portable storage device as soon as possible after its use.
- Disable automatic Wi-Fi connections (external to the SRCE system).
- Do not take SRCE-provided devices outside of Canada unless you have prior written special approval from the Regional Executive Director of Education.

General Cautions

- Do not leave personal information on a message machine. Simply leave a message to return your call.
- Do not discuss personal information in any area where the conversation may be overheard by unauthorized personnel (e.g., staff room, hallway).
- Apply the principle that staff should have access only to the personal and sensitive information on a 'need-to-know' basis that they require to fulfill their work responsibilities.
- Write professionally and respectfully.
- Write factually and avoid opinions unless based on facts.
- Marking 'confidential' does not make it so. It is all in the intent and the content.

Questions

- If you have any questions about information access and privacy, please contact SRCE Information Access and Privacy staff:
  - Deanna Gillis; 902-625-7093; deanna.gillis@srce.ca
  - Cheryl MacPherson; 902-625-7065; cheryl.macpherson@srce.ca