PURPOSE

This guideline defines and recommends best practices for managing recorded confidential records and information held by school boards/authorities. Following these practices will help to prevent breaches of privacy, security, or confidentiality. School boards/authorities should use this guideline to develop their own practices and procedures governing confidential records and information management.

Confidential

Recorded confidential records and information management refers to records and information that must be maintained in confidence and must not be disclosed unless authorized. Confidential records and information management includes but is not limited to private personal information. Confidentiality as a concept applies to a duty to protect records and information and can be applied to various types of records and information, not just personal records and information.

Disclosure of recorded confidential records and information should be limited to specific people or groups for a specific purpose. For example, this means that employees who require confidential records and information in the performance of their assigned duties–or, in the case of personal records and information, with the consent of the individual to whom the records and information relates–can indeed have it.

The Legal Framework

The *Ontario Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) provides a framework for determining which records and information may be considered as personal and/or confidential. The *Education Act* sets out, among other things, which information causes trustee meetings to be held in private session and which student information is private.

Personal and Confidential Records and Information

School board/authority records and information that may be confidential includes:

- a draft of a by-law;
- records and information revealing the substance of deliberations of a closed meeting, provided the closing of the meeting to the public is authorized by statute (*Education Act*);
- advice or recommendations of an officer or employee of an institution or a consultant retained by an institution;
- records and information received in confidence from government;
- records and information that disclose a trade secret or scientific, technical, commercial, financial, or labour relations records and information, supplied in confidence implicitly or explicitly (information falling in this definition must be treated as confidential in the absence of consent from the third party who provided it to the school board/authority;

- records and information that may be protected by legal privilege which includes:
  - communications between solicitor and client for the purposes of furnishing or obtaining legal advice (solicitor/client privilege);
  - records prepared in contemplation of or for use in litigation (litigation privilege); and
  - records prepared by or for legal cousel for use in giving advice.
- records and information protected by statutory privilege, i.e., the *Education Act* applies a statutory privilege to the Ontario Student Record (OSR) which restricts its use to the principal, superintendent, and teachers of the school for the improvement of the instruction of the pupil, unless consent is given by the adult student or the parent of the minor student for its broader use and disclosure;
- records and information collected by a health professional (e.g., psychologist, social worker, therapist) and/or clergy where specific circumstances are met;
- records and information that may pose a danger to safety or health; records and information that could reasonably be expected to seriously threaten the safety or health of an individual; refusing to disclose records and information to a parent when precluded to do so by court order or when in the principal's judgment there is an immediate risk of harm to a student.
- law enforcement records and information/proceedings (may include administrative tribunals);
- economic and other school board/authority interests, including:
  - trade secrets or financial, commercial, scientific, or technical records and information of a vendor or of the school board/authority;
  - records and information obtained through research by an employee, if the disclosure could reasonably be expected to deprive the employee of priority of publication;
  - records and information whose disclosure could reasonably be expected to prejudice the economic interests or the competitive position of the school board/authority;
  - records and information whose disclosure could reasonably be expected to be injurious to the financial interests of the school board/authority;
- positions, plans, procedures, criteria, or instructions to be applied to any negotiations carried on or to be carried on by or on behalf of the school board/authority;
- plans relating to the management of personnel or the administration of the school board/authority that have not yet been put into operation or made public;
- proposed plans, policies, or projects of the school board/authority if the disclosure could reasonably be expected to result in premature disclosure of a pending policy decision or undue financial benefit or loss to a person;
- questions that are to be used in an examination or test for an educational purpose.

Personal Information

Personal information is defined by MFIPPA as recorded information about an identifiable individual and should be treated as confidential unless it is public information or unless the individual consents to its disclosure or disclosure of the information is otherwise permitted by MFIPPA. For example, under MFIPPA, public information includes information that identifies an individual in a business or official capacity.

Personal Health Information which is a category of personal information should also be treated as confidential in accordance with the Personal Health Information Protection Act (PHIPA) where appropriate.

Identifying and Labeling Recorded Confidential Records and Information

Confidential records and information must be identified and clearly marked to ensure that staff can apply appropriate protection measures to the records and information. Marking may be done by including "CONFIDENTIAL" in the header or footer or as a watermark on all documents. Additionally, confidential documents or reports may be photocopied on coloured paper designated for that purpose, e.g., minutes of closed session on blue paper. Distribution or circulation of the documents may be restricted by including which persons may use the documents on each document, e.g., CONFIDENTIAL - for the use of the Board of Trustees only.

Only records that meet the criteria for confidential records and information should be marked as such. The following are some examples of confidential records and information:

- Reference letters
- Ontario Student Records
- Personnel records
- Evaluations of performance
- Health records
- Grievance files
- Appeal files
- Payroll records

When Could Records and Information Cease to Be Confidential?

Some confidential records and information may only be sensitive for specified periods, ceasing to be confidential after a certain period of time or change of circumstances. Here are some examples:

- RFP submissions.
- Draft press releases.
- Restructuring plans, policies, or projects.
- Personal information where it is about a person who has been dead for more than 30 years.

Access to Confidential Records and Information

Access to recorded confidential records and information is determined by the content of the records and information. MFIPPA allows an employee or agent of the organization who needs the records and information in the performance of his/her duties to have access to personal and confidential records and information on a limited, need-to know basis. School boards/authorities should assess the duties and responsibilities of each role to determine what information the staff member should be granted access to. Access to personal information should be minimized as much as possible to reduce risk.

Guidelines to Protect Confidential Records and Information

The following guidelines should be considered for confidential records:

- Access to the confidential records should be restricted only to those employees that require the records and information in the performance of their assigned duties.
- Include "confidential" in the header or footer or as a watermark or stamp for each document containing confidential records and information.
- Photocopying confidential reports on a coloured paper designated for that purpose, e.g., closed session minutes and agendas on blue paper.
- Keeping records in a secure location, such as in locked file cabinets, in locked rooms, or on a secure server. Cabinets should always be kept locked when not in use and located in a private/secure area, and access to the cabinets should be limited to authorized employees.
- Confidential records and information should be placed in a file folder, envelope, or other form of cover when out of the secure cabinet. When the record is not in use, it should be returned to the cabinet right away.
- Confidential records and information should never be left in an open area such as in an in-basket or on a desk. The record should be returned to the cabinet when not in use.
- Confidential records and information must be destroyed by secure shredding or by other secure data destruction methods.
- Confidential records and information should be stored separately from other similar records to support controlled access.
- For electronic records, store confidential records in separate directories or files, restrict access to these directories or files, and remove by secure deletion only.
- Computer screens should be positioned to prevent unauthorized viewing.
- Use passwords to protect confidential records and information and protect your passwords (see Password Guidelines).
- Shut down programs or use password protection on your computer when you leave your desk.
- Turn off your computer when leaving your desk for a long period of time.
- Shred drafts when they are no longer useful, and delete drafts from your computer.

- If you have confidential records on a notebook or laptop computer, ensure that either the documents themselves or the system are password protected. Do not leave your laptop in an easily accessible area where it could be stolen. Consider using data encryption for protected confidential records and information on portable devices.
- When travelling with confidential records, do not leave them unattended in vehicles, hotel or meeting rooms. Do not work with confidential records where others can see them.
- Do not remove Ontario Student Records from the school.
- If confidential records and information must be faxed, include a fax transmittal page with a confidentiality statement. Verify that the number on the screen is accurate before proceeding with the transmission, and confirm receipt of the documents.

Guidelines for the Secure Disposal of Confidential Records and Information

Confidential records and information must be disposed of securely to ensure they are permanently destroyed or erased in an irreversible manner and by a method that ensures that the records cannot be reconstructed in any way. When disposing of confidential records and information, official files as well as duplicate copies of documents made for in-office use should be considered.

- Paper - destruction means cross-cut shredding; this method is preferred to strip shredding, from which documents may be reconstructed. Consider whether on-site or off-site destruction is more suitable for your organization.
- Electronic and wireless media (such as floppy disks, CDs, USB keys, personal digital assistants (PDAs), and hard drives) - destruction means either physically damaging the item (rendering it unusable) and discarding it, or, if re-use within the organization is preferred, this entails employing file-wiping utilities provided by various software companies. Wiping may not, however, irreversibly erase every bit of data on a drive (see Information Technology Equipment Hardware Disposal and Redistribution Guidelines).

Resources

For more information on disposing of confidential records and information, refer to the Information and Privacy Commissioner of Ontario's Fact Sheet Number 10, *Secure Destruction of Personal Information*, available at http://www.ipc.on.ca/images/Resources/up-fact_10_e.pdf.

References

Information and Privacy Commissioner of Ontario's Fact Sheet Number 10, *Secure Destruction of Personal Information*, available at http://www.ipc.on.ca/images/Resources/up-fact_10_e.pdf.

York University, *Tip Sheet 2: Confidential Records*, available at http://www.yorku.ca/secretariat/infoprivacy/infotoolkit/docs/TipSheet2ConfidentialRecords.pdf.

Athabasca University, Guidelines - *Confidential Records and Information*, available at http://www.athabascau.ca/foipp/guidelines/guideline3.html.