Strait
Regional Centre for Education

Privacy 101: Accessing Personal Information on a Need-to-Know Basis Only

Accessing Personal Information on a Need-to-Know Basis

In accordance with the Student Records Policy and applicable privacy legislation, employees may only access the personal information of others on a **need-to-know basis**.

When access is considered on a “need-to-know” basis, need-to-know is determined by relevancy for delivery of programming and provision of services and safety and security of students, staff, and members of the school community; and must pertain to one's work responsibilities.

Employee Responsibilities

- Employees shall not access the information of an individual or individuals out of curiosity, just because “they can” or for some other unauthorized reason. Viewing personal information without a specific authorized purpose is strictly prohibited and considered a privacy breach, whether or not the intent was malicious. It also does not matter what format the information is in when it is accessed or whether the information acquired was used or disclosed for any reason.
- While it may seem harmless to access the information of family/friends/co-workers, even at their request, it is important to treat all individuals equally and follow the same access procedures for consistency, fairness and record keeping purposes.
- When accessing a record for a work-related reason, all employees are responsible for only accessing, collecting, using and disclosing the minimum amount of information needed to do your job.
- This means limiting access, use, disclosure or requests for personal information to only the amount required and that the information is shared only with those who have a valid need to know.
- The easiest way to avoid accidental, unauthorized access to personal information is to use access you have only for purposes directly related to your job duties.
- Everyone is responsible to report if they have discovered or suspect unauthorized access is occurring. Unauthorized access to personal information is considered a privacy breach; all breaches, suspected or actual, must be reported to a supervisor or privacy designate (IAP administrator) to be managed accordingly.
- If a situation occurs where you are required to access the information of someone known to you, it is advisable to report the conflict to your supervisor and have them decide if the task should be re-assigned.

Strait
Regional Centre for Education

Privacy 101: Accessing Personal Information on a Need-to-Know Basis Only

Examples of Intentional and Unauthorized Access of Personal Information

- A relative asks you to check on the status of their employment application in a system to which you have access.
- You saw your neighbour come into your place of work and were curious about what they were doing there, so you asked a colleague or looked them up in a database.
- There was an interesting story about someone on the news and you want to see if you can find out more about them by searching your system.

Unauthorized Access to Information Considerations

- It may start innocently, with someone looking up their own information and then expanding that search to family and friends and eventually moving to others.
- Even if an individual requests their own personal information from the government and gives their consent, it is still considered unauthorized access if the proper procedure to access the information is not followed. For example, a neighbour that knows you work with a government database asks for their own information without following the proper application process.
- If personal information has been posted or shared publicly, such as on a person's social media, it does not give the right to look it up in a database to which you have access.
- Close relationships do not grant the right to look up information. Viewing the information of friends, siblings, family members or spouses can all be considered unauthorized access if there is not a specific authorized purpose for the access.

Caution Understanding the Risks

- The unauthorized access of personal information impacts public trust in the organization, it undermines the public's confidence in the ability of a public body to protect their personal information and may hurt, humiliate or bring reputational damage to any affected individuals.
- The unauthorized access of personal information may have personal penalties, such as disciplinary action or negative consequences, such as financial penalties, for government for violating privacy obligations.

Resources

- Students Records Policy
- Provincial Privacy of Student Information Policy
- Freedom of Information and Protection of Privacy (FOIPOP) Act
- Application legislation and collective agreements