NIAGARA CATHOLIC
DISTRICT SCHOOL BOARD

Administrative Operational Procedures for Working Outside of the School/Office

March 2020

Table of Contents

1. Introduction

- In the course of performing their duties, Niagara Catholic District School Board (the *Board*) employees may be required to work outside their conventional school or office space. This may include transporting records by car; working on assignments or projects at home; attending meetings and conferences; appearing at court or tribunal hearings; conducting investigations; making visits to other schools or offices of other service providers.

- Records containing personal information may be either in paper or electronic format. The purpose of these guidelines is to set out how employees must protect the privacy and confidentiality of such records when working outside their conventional school or office space.

- Board employees are expected to familiarize themselves with these guidelines and are reminded of their related professional obligations to promote public trust and confidence in the education system.

2. Other Sensitive Information

- In certain circumstances, employees who are working outside the school/office may be dealing with other confidential records that do not necessarily include personal information, such as purchase agreements, records subject to solicitor-client privilege, or records containing advice from government. Although these guidelines apply to personal information, they are equally applicable to records containing other types of sensitive information.

3. Freedom of Information and Protection of Privacy Legislation

- When working both inside and outside the school/office, Board employees must comply with the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*). One purpose of the *Act* is to protect the privacy of individuals with respect to personal information about themselves held by the Board.

- Personal information is defined in the *Act* as recorded information about an identifiable individual, including his or her race, age, family status, address, telephone number, educational, medical or employment history and other information. The *Act* contains privacy rules governing the collection, retention, use, disclosure and disposal of personal information held by the Board. For further details, consult the full text of the *Act*, which is available online: *https://www.ontario.ca/laws/statute/90m56*

4. Removing Records from the School/Office

- Employees must only remove records containing personal information from the school/office when it is necessary for the purposes of carrying out their job duties. If possible, only copies should be removed, with the original hard copies left in the school/office.

- Employees are required to obtain approval from their supervisor/principal before removing records containing personal information from the school/office.

- Records containing personal information that are being removed from the school/office must be recorded on a sign-out sheet that includes the employee's name, a description of the records; the names of the individuals whose personal information is being removed; and the date the records were removed.

5. Paper Records

- Paper records containing personal information must be securely packaged, carried in a locked container or sealed box, and kept under the constant control of the employee while in transit.

- When an employee travels by car, paper records must always be locked in the trunk. Consequently, unless there is no alternative, paper records must never be left unattended in a car trunk while the employee goes elsewhere.

- Paper records must not be opened or reviewed while travelling on public transportation such as a taxi, bus, train, or airplane.

- When working at home, paper records must be stored in a locked cabinet or desk drawer when they are not being used. The cabinet or desk must only contain work-related records.

- When working at other locations outside the school/office, paper records must be kept under the constant control of the employee, including during meals and other breaks. If this is not possible, the records should be temporarily stored in a secure location, such as a locked room or desk drawer.

6. Electronic Records

- Employees must remotely access electronically available records when working outside the office/school. Employees must refrain from making printed copies to work off-site.

- Employees must refrain from saving personal information to a portable device such as USB/Memory Sticks/Jump Drives. Files should be saved using Board endorsed cloud platforms: G-Suite and O365 and DocuShare.

- If a record is too large to send electronically and it needs to be saved temporarily to a portable device, employees must delete the information as soon as it has been transferred to the recipient.

- To prevent loss or theft, the portable device must be carried in a locked container and kept under the constant control of the employee, including during meals and other breaks. If this is not possible, they must be temporarily stored in a secure location, such as a locked room or desk drawer.

7. Laptops, Notebooks and Home Computers (Computers)

- Computers used to access personal information while working outside of the office/school, including home computers, must be password-controlled.

- Computers must be kept under the constant control of the employee while in transit. When an employee travels by car, a computer must always be locked in the trunk. There have been cases, however, where computers have been stolen from employees, including from the locked trunk of a car. Consequently, unless there is no alternative, computers must never be left unattended in a car trunk while the employee goes elsewhere.

- If it is necessary to view personal information on a computer screen when working at locations outside the school/office, ensure that the screen cannot be seen by anyone else. Personal Information should never be viewed on a computer screen while travelling on public transportation.

- When working at home or at other locations outside the school/office, computers must be logged off and shut down when not in use. To the maximum extent possible, the employee must maintain constant control of the computer, particularly when working at locations outside the school/office other than home. If this is not possible, it must be temporarily stored in a secure location, such as a locked room, cabinet or desk drawer.

- Do not share a computer that is used for work purposes with other individuals, such as family members or friends.

8. Wireless Technology

- Employees must protect the privacy and confidentiality of personal information stored on wireless devices such as tablets and cell phones. Access to such devices must be password-controlled, and any stored data should be encrypted.

- To prevent loss or theft, a wireless device must be carried in a locked briefcase or closed purse and kept under the constant control of the employee while in transit. Never leave a wireless device unattended in a car. If it is absolutely necessary to view personal information on a wireless device while in public or when travelling on public transportation, ensure that the display panel cannot be seen by anyone else.

- When working at locations outside the school/office, the employee must maintain constant control of wireless devices. If this is not possible, they should be temporarily stored in a secure location, such as a locked room, cabinet or desk drawer.

- Do not share wireless devices that are used for work purposes with other individuals, such as family members or friends.

9. Telephones and Voice Mail

- When located in public areas, including on public transit, employees must avoid using cell phones to discuss personal information. Listening to voicemail may also be overheard by individuals close by and must be avoided.

- Employees must not provide home phone numbers as a contact number for work related business. Family members may inadvertently pick-up a call or listen to a voice mail message that involves personal information they are not authorized to access.

10. Conversations Outside the School/Office

- Employees must not discuss personal information in public locations such as public transit, restaurants, retail stores or on the street. If it is necessary to do so, move to a location where other persons cannot overhear your conversation.

11. Reporting Requirements

- The loss or theft of personal information/suspected privacy breaches must be reported immediately to an employee's supervisor, or, in their absence, the appropriate Superintendent or the Coordinator of Information Management/Privacy and Freedom of Information.

- Employees will be asked to provide a list of all the personal information that may have been compromised in the event of a breach.

- Employees will be asked to provide details about the breach and measures they had taken (as per these guidelines) to protect the personal information in their care and custody.

Niagara Catholic's Privacy Breach Procedure

Niagara Catholic's Privacy Policy

Top 5 Tips for Avoiding a Privacy Breach When Working from Home