Administrative Procedure 180 – Appendix A

GUIDELINES FOR PROTECTING THE PRIVACY AND CONFIDENTIALITY OF PERSONAL INFORMATION

Background

In the course of performing their duties, employees may be required to work outside their regular office space or school. This may include transporting records by car and other transportation methods; working on assignments or projects at other school division locations; attending meetings at hotels and conference centres; and representing the school division at ceremonies or public gatherings.

Records containing personal information may be in paper and/or electronic format including student files, assessment protocols, student reports, laptops, cell phones, tablets/iPads, professional notes, and external drives. The purpose of these guidelines is to set out how employees should protect the privacy and confidentiality of such records when working outside the office.

Whenever personal information is being used outside of the office there is an increased risk that it may be lost or compromised. In the course of performing their duties, Prairie South School Division employees must take reasonable measures to keep paper and electronic records safe and secure.

Procedures

1. Freedom of Information and Protection of Privacy Legislation

1.1. When working both inside and outside the office, employees must comply with The Local Authority Freedom of Information and Protection of Privacy Act (LAFOIP). One purpose of the Act is to protect the privacy of individuals with respect to personal information about themselves held by the school division.

1.2. Personal information is defined in the Act as recorded information about an identifiable individual, including his or her race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual, and other information.

2. Removing Records from the Office

2.1. Employees should only remove records containing personal information from the office when it is absolutely necessary for the purposes of carrying out their job duties. If possible, only copies should be removed, with the originals left in the office. If using original documents, remove only relevant documents or extract a summary and return them as quickly as possible. When copies are no longer needed, they should be destroyed in a secured manner (shredded).

2.2. Depending on their positions, employees may be required to obtain approval from their supervisor before removing records containing personal information from the office.

2.3. Records containing personal information that are being removed from the office should 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.

2.4. Procedures for transporting Student Cumulative Files are outlined by the Ministry of Education in the Student Cumulative Record Guidelines document.

3. Paper Records

3.1. Paper records containing personal information should be securely packaged in folders, carried in a locked briefcase or sealed box, and kept under the constant control of the employee while in transit.

3.2. When an employee travels by car, paper records should always be locked in the trunk. If storing the information overnight, the information should be stored as above, in a locked garage or inside the house if no garage exists.

3.3. Paper records should not be opened or reviewed while travelling on public transportation such as a bus or airplane.

3.4. When working at other locations outside the office, paper records should 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.

4. Electronic Records

4.1. Electronic records containing personal information should be stored and encrypted on a password-protected flash drive rather than the hard drive of a laptop or home computer.

4.2. To prevent loss or theft, the flash drive must to be kept under the constant control of the employee while in transit.

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

5. Laptop and Home Computers

5.1. Access to laptop and home computers should be password-controlled, and any data on the hard drive should be encrypted. Other reasonable safeguards, such as anti-virus software and personal firewalls, should also be installed.

5.2. Laptops should be kept under the constant control of the employee while in transit. When an employee travels by car, a laptop should always be locked in the trunk.

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

5.4. When working at home or at other locations outside the office, a laptop or home computer should be logged off and shut down when not in use.

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

6. Wireless Technology

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

6.2. To prevent loss or theft, a wireless device should kept under the constant control of the employee while in transit. Never leave a wireless device unattended in a car. If it is 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.

6.3. When working at locations outside the office, the employee should 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 or desk drawer.

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

7. Faxes and Photocopies

7.1. Ideally, employees should undertake the faxing or photocopying of personal information themselves. However, in some locations outside the office, fax and photocopy machines for individual use may not be readily available. If employees must submit records containing personal information to a third party for faxing or photocopying, they should ask to be present when these tasks are being done.

7.2. It is required that all staff sending confidential information include the following statement as part of their fax cover sheet:
This fax and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. This message contains confidential information and is intended only for the individual named. If you are not the named addressee, you should not disseminate, distribute or copy this fax. Please notify the sender immediately by email or telephone if you have received this fax by mistake and destroy this fax. If you are not the intended recipient, you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

7.3. Before faxing personal information, employees must confirm that they have the correct fax number for the intended recipient.

7.4. When faxing personal information, employees must stay by the machine to ensure that all materials were transmitted correctly.

8. E-mail

8.1. It is required that all staff sending confidential information include the following statement as part of their email signature:

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. This message contains confidential information and is intended only for the individual named. If you are not the named addressee, you should not disseminate, distribute or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. If you are not the intended recipient, you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

8.2. Limit all personal identifiers and confidential information before emailing the information, wherever possible. It is recommended for attachments the document is password protected and the password will not be shared in the same email.

8.3. Before emailing personal information, confirm that you have the correct email address for the intended recipient.

9. Working Remotely with Personal Information

9.1. If you will be working with personal information from home or remotely, take care to make sure you are the only person able to access the records. Simple steps to take include:

9.1.1. Log off or shut down your laptop or home computer when you are not using it.

9.1.2. Set the automatic logoff to run after a short period of idleness.

9.1.3. Do not share a laptop used for working with personal information with other individuals, including family members and friends.

9.1.4. When records are not being used, store in a secure location.

9.1.5. Avoid sending personal information by fax from public locations.

10. Using Personal Smartphones for Work Related Purposes

10.1. This procedure also applies if you are using your own device for work purposes. If personal information is stolen or lost, you must report the incident in accordance with the reporting requirements clause.

11. Reporting Requirements

11.1. When confidential information is lost, compromised or potentially compromised, contact your supervisor immediately. The Supervisor will immediately report the incident to the LAFOIP Officer of the school division. The Officer will notify the Office of the Saskatchewan Information and Privacy Commissioner.

11.2. The school division will notify the individuals whose personal information has been stolen or lost, telling them the kind of information that has been compromised and steps that are being taken to recover it.