PURPOSE

This guideline reflects best practices for securing personal information when working outside of the office or school. When working away from the school or office, records may be removed from the office or created off-site. This raises concerns about the privacy and confidentiality of records.

Overview

When personal information is in the care and/or custody of school board/authority employees they are responsible for ensuring that the information is protected and privacy is not breached.

This applies to records and information in all formats (paper, computer, photos, drawings, recordings, etc.).

Employees working off-site often convey information and records through various means including technology. In particular, technology has a significant impact on how records are handled and on how personal and other information is collected, stored, and communicated.

While this technology is efficient, it may diminish the confidentiality of the information transmitted. For that reason, the Information Privacy Commissioner suggests that institutions encourage employees take special care when using technology.

Guidelines

Refer to the following guides found within the toolkit for more detail:

1. Guidelines for Password Procedures

2. Guidelines for the Securing Mobile Devices

3. Technical Guidelines for Data Encryption

4. Considerations for the Use of Electronic Records in Place of Paper

5. Information Technology Equipment Hardware Disposal and Redistribution Guidelines

6. Privacy Breach Protocol

Recommendations

- Mobile technologies used outside the office include laptop computers, jump drives, cell phones and PDAs. Any technology that has sensitive information stored on them must be secure at all times.

- Sensitive information should not be stored on mobile devices if possible.

- Sensitive information, if stored on mobile devices, should be:

  - securely encrypted

  - a copy — not the only instance of the data

- Sensitive information should always be transmitted in a securely encrypted format and never by email.

- Portable devices and storage media with sensitive information should be destroyed or erased so there is no possibility of subsequent data recovery.

- Original records with sensitive information should not be removed from the work site.

Considerations for protecting records when working offsite

- Whenever practical, the original should remain on-site and only copies removed. Copies should be clearly identified as such and shredded when no longer needed.

- Utilize a sign-in/sign-out procedure with a due-back date to monitor removed files. Whenever possible, remove only relevant documents or an extract or summary.

- Return records to a secure environment as quickly as possible, for example, at the end of a meeting, the end of the day, or the end of a trip.

- Retain all working copies according to your institution's records retention schedule, or disposed of in a secure manner so that the record may not be reassembled and read.

- Records containing personal or confidential information should never be discarded in a client's or a public trash or recycling bin.

- Records should not be left unattended and, where possible, should be physically locked away or secured.

- Records in any format should be transported as carry-on luggage whenever travelling by commercial carrier unless the carrier requires otherwise.

- Do not leave paper records or mobile devices containing personal information in your vehicle. (If it absolutely cannot be avoided, lock them in your trunk before you start the trip, not in the parking lot of your destination or other visible location. If the vehicle does not have a trunk, leaving the device in the vehicle is not a secure option.)

- All paper records and mobile devices should be discreetly and permanently marked as school board/authority property and indicate a method of return in case the device is lost.

- While viewing personal information at locations outside the office, ensure that it cannot be seen by anyone else.

Working from Home

Designate a secure work area as "office space."

If possible, and where appropriate, install a second telephone line dedicated to work-related calls. This is particularly important for employees who need a phone line for a fax or modem. If an answering machine or answering service is required, ensure work-related messages can be accessed only by the employee. It is advisable to have a machine separate from that of the household or to use a password different from the household's to access work-related messages from an answering service.

Employees should store all paper and electronic records in the most secure fashion available.

Cell Telephones

Avoid using cell phones to discuss personal information. Cell phone conversations can be easily overheard or intercepted by individuals using scanners or other devices.

When making telephone calls from outside the office, employees should safeguard personal and confidential information as much as possible. For example, consider the physical setting to ensure that no one overhears a telephone conversation.

References

Kansas Sate University, Information and Privacy Commissioner Office