Operational Guidelines

Category: Privacy

Privacy Guidelines Working from Home

Introduction:

Algoma Family Services (AFS) is committed to keeping personal information under its custody and control, safe and secure, at all times, especially in the event that employees are required to work outside of the office.

PURPOSE:

The purpose of these guidelines is to set out how employees should protect the privacy and confidentiality of records when working outside the office. This may include transporting records by car, bus, subway, train or airplane; working on assignments or projects at home; attending meetings at hotels and conference centres; appearing at court or hearings; making visits to clients; and representing AFS at ceremonies or public gatherings.

PROCEDURES:

Personal information is defined as recorded information about an identifiable individual, including his or her race, age, family status, address, telephone number, medical or employment history and other information.

RECORDS

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.

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

When an employee travels by car, paper records should always be locked in the trunk. Paper records should never be left unattended in a car trunk while the employee goes elsewhere.

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

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.

LAPTOPS/COMPUTERS

Access to laptop and home computers should be password-controlled.

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. Laptops should never be left unattended in a car trunk while the employee goes elsewhere.

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.

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. To the maximum extent possible, the employee should maintain constant control of the laptop, particularly when working at locations outside the office other than home. If this is not possible, it should be temporarily stored in a secure location, such as a locked room or desk drawer.

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

WIRELESS TECHNOLOGY

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.

To prevent loss or theft, a wireless device should be 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.

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

When in transit or working outside the office, employees should avoid using cell phones to discuss personal information. Cell phone conversations can be easily overheard.

FAXES/PHOTOCOPIES

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.

CONVERSATIONS OUTSIDE THE OFFICE

Employees should not discuss personal information in public locations such as buses, commuter trains, subways, airplanes, restaurants, or on the street. If it is necessary to do so, move to a location where other persons cannot overhear your conversation.

REPORTING REQUIREMENTS

The loss or theft of personal information should be reported immediately to the immediate supervisor and the Information & Privacy Coordinator.