Regina Open Door Society

Privacy Policy &

Security and Safety Guidelines

PRIVACY POLICY & SECURITY AND SAFETY GUIDELINES

1 PRIVACY POLICY PRINCIPLES

1.1 LEGAL PROTECTIONS FOR PERSONAL INFORMATION

The *Freedom of Information and Protection of Privacy Act* (FOIP Act) sets the legal authority and ground rules for our collection, use and disclosure of personal information for the direct client services. This privacy policy document describes how we protect the personal information we collect, use and disclose in accordance with the FOIP Act. This policy also complies with *Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) requirements.

1.2 OUR PRIVACY AND CONFIDENTIALITY COMMITMENT

We have to collect, use and disclose some personal information about our clients to deliver services. Protecting their personal information is one of our highest priorities. We are responsible for personal information in our possession or custody.

This document describes how our privacy commitment is reflected in our activities. It applies to our organization, our employees and to any person providing services on our behalf. We have posted a copy of our privacy policy on our web site and copies are available in our offices. We will provide a copy to anyone on request.

1.3 WHAT IS PERSONAL INFORMATION?

Personal information is recorded information about an identifiable individual, as defined in Section 24 of the FOIP Act. Personal information includes such things as name, gender, birth date, where the individual lives, the individual's home, cell, business and fax numbers, e-mail address, marital status, photos and unique personal identifiers assigned to that individual, such as a social insurance number, driver's license number, credit card number or a file number. It also includes other information about an identifiable individual contained in case files or any other records.

Recorded information includes any information that is written, photographed, recorded or stored in any manner, but does not include computer programs or other mechanisms such as a photocopier or fax machine that copy records.

1.4 WHAT PERSONAL INFORMATION WE COLLECT

We only collect the personal information necessary to provide the services that best meet client needs. We do not collect personal information that is "nice to know" or "just in case we might eventually need it".

1.5 HOW WE COLLECT PERSONAL INFORMATION

We normally collect client personal information directly from our clients. Sometimes we may collect client personal information from other persons or organizations, with client consent or as authorized by the FOIP Act.

When we collect personal information, our clients have a right to know why we are collecting their personal information, what we will be using it for, and who may see it. We will inform our clients, before or at the time of collecting personal information, of the purposes for which we are collecting the information.

If someone asks a question about the purpose for the collection, use or disclosure of information, we will provide an answer or refer the client to someone who can. We have designated a privacy contact person who can help our staff and assist with client questions or requests, as needed.

1.6 NOTICE AND CONSENT

Our funding agreements require that we share certain information about our clients. We provide notice of the information that may be disclosed and request the client's authorization for the disclosure. We may be unable to provide services if this authorization is refused.

Except when required by our funding agreements or by law, written client consent is required before we provide personal information to outside agencies or individuals. If we refer a client to another service provider, before sharing any information with that service provider we will get the client's written consent. We will not share client information with any person or organization outside those listed in the written consent, except as required by our funding agreements or by law.

A client may withdraw consent to the use and disclosure of personal information at any time, unless the personal information is necessary for us to fulfill our obligations under law or our funding agreements. We will respect a client's decision, but we may not be able to provide certain services if we do not have the necessary personal information. A withdrawal of consent cannot be retroactive; that is, it cannot be applied to actions taken in the past.

1.7 ENSURING ACCURACY OF CLIENT INFORMATION

When we collect information about a client, we make every reasonable effort to ensure that the personal information we collect is accurate and complete. We want to prevent using wrong or inaccurate information to make a decision about a client.

We rely on clients to tell us if there is a change to their personal information that may affect the services they receive.

1.8 HOW WE USE AND DISCLOSE PERSONAL INFORMATION

We only use and disclose a client's personal information for the purposes for which the information was collected, or for purposes that are clearly consistent with the original purposes. If we wish to use or disclose a client's personal information for any other purposes, we will ask for client consent before doing so.

1.9 HOW WE KEEP PERSONAL INFORMATION SAFE

We make every reasonable effort to protect all personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks, using measures appropriate for the sensitivity of the information.

1.10 ACCESS TO RECORDS CONTAINING PERSONAL INFORMATION

Clients have a right to access their own personal information in our records, subject to a few specific exceptions in law. Such access may be subject to procedures or conditions associated with the processing of such requests, including proof of identity.

1.11 RIGHT TO REQUEST CORRECTION

Clients may request correction of any errors or omissions in their factual personal information by making a request in writing. We can correct factual errors whenever we are notified of them. In some cases we may ask for verification.

If the request is to change information that reflects a professional opinion or assessment, the request will be directed to our designated privacy contact person. We may be limited in our ability to change information that reflects a professional opinion or evaluation.

1.12 QUESTIONS AND COMPLAINTS

If clients have a question or concern about any collection, use or disclosure of their personal information by us, or about a request for access to their own personal information, or our compliance with this privacy policy, they should contact our designated privacy contact persons first.

Gratta Nimbeshaho
Manager of the Newcomer Welcome Centre
Regina Open Door Society
306-352-5775

Or

Samantha Gardiner
Human Resources Coordinator
Regina Open Door Society
306-352-3500

Clients always have the option to contact the Office of the Saskatchewan Information and Privacy Commissioner for questions and concerns about their personal information.

Saskatchewan Information and Privacy Commissioner
503 – 1801 Hamilton Street Regina, Saskatchewan S4P 4B4
Telephone: (306) 787-8350 Toll Free Telephone (within Saskatchewan): 1-877-748-2298

2 PRIVACY POLICY STATEMENTS

2.1 RODS (REGINA OPEN DOOR SOCIETY) RESPONSIBILITIES

P1. We are responsible for personal information in our possession or custody.

P2. We will make our employees and any person providing services on our behalf, including volunteers and contractors, aware of their privacy responsibilities when their employment commences and before they start collecting and using personal information.

P3. We will communicate all changes to the privacy policy to employees as soon as possible after the changes occur.

P4. We will post a copy of the privacy policy on our web site and make copies available in our office(s).

P5. We will make employees aware that the FOIP Act includes offences and substantial penalties for intentional contravention of the Act:

> *"Every person who knowingly collects, uses or discloses personal information in contravention of this Act or the regulations is guilty of an offence and liable on summary conviction to a fine of not more than $1,000, to imprisonment for not more than three months or to both fine and imprisonment*." [FOIP s.68(1)]

P6. We will designate a privacy contact person who can advise employees with privacy-related questions and assist with client requests, as needed.

P7. We will provide information resources to help employees incorporate good privacy practices into their work activities.

2.2 EMPLOYEE RESPONSIBILITIES

P8. Employees are responsible for compliance with this privacy policy.

P9. Employees will be asked to sign a confidentiality oath, acknowledging that they have read and understand the privacy policy.

P10. Employees are required to review the privacy policy at least annually.

P11. Failure to comply with the privacy policy may result in disciplinary action, up to and including termination.

2.3 NOTICE AND CONSENT

P12. Clients shall be provided notice of the purposes of any personal information disclosures and the recipients of any disclosures made necessary by RODS (Regina Open Door Society) funding agreements, or by related legislation. Clients will be asked to sign an authorization for such disclosures.

a) For all other disclosures of personal information outside RODS, a client must freely consent in writing before such a disclosure can take place. Such disclosures may include, but are not limited to, sharing information with another service provider or disclosure for a purpose different than that for which the information was originally collected.

   i) The signed form must be placed in the client's file.

P13. A client's representative may provide written consent on behalf of the client, but only if the client is unable to do so.

P14. The provision of consent on behalf of the client by a representative is subject to P26 below.

P15. For the collection, use and disclosure of personal information by RODS in line with the stated purposes verbal consent is acceptable if it is provided by the client or the client's representative and if the consent is noted and dated on the client's file.

P16. Client consent cannot be the only authority for the collection of personal information. The collection of personal information must be for a purpose that relates to an existing or proposed program or activity of the organization.

P17. Explicit client consent may authorize the use or disclosure of personal information for purposes different than the purposes for which the personal information was collected.

P18. A client may withdraw consent for the collection, use or disclosure of his or her personal information at any time.

a) The withdrawal of consent must be in writing.
b) The withdrawal of consent must take effect on a specific current or future date. Consent cannot be withdrawn for a date in the past.
c) The client shall be informed of any services that might not be available as a result of a withdrawn consent, before the consent is withdrawn.

2.4 COLLECTION OF PERSONAL INFORMATION

P19. Employees must collect only the information that is necessary to provide services to the client at the time of collection, or for services that may be reasonably anticipated at the time of collection. Information that would be “nice to know”, “might be useful at some future time”, or simply to fill in a space on an intake form or a field in the information system must not be collected.

P20. If there is uncertainty whether information should be collected, employees must seek advice from the designated privacy contact person prior to collection.

P21. Clients must be informed at or before the time of collecting personal information, of the purposes for which we are collecting, using and disclosing a client’s personal information.

P22. We will display a brochure that explains the purpose and privacy implications of collecting client information. The brochure will be kept in a location visible to all clients for their easy access.

P23. If a client has questions about the collection of their information, employees shall respond to informal client information requests, and if required, contact the designated privacy contact person for advice.

P24. The client must be asked to sign an informed consent form at the time of first collection of personal information.

P25. Whenever feasible, personal information must be collected directly from the person to whom it relates.

P26. If direct collection from the client is not feasible, the following options are available:

a) Personal information may be collected from the client's interpreter/translator, companion or relative, if the client is present at the time of collection.

b) If the client is not present at the time of collection, any person providing personal information or consent on a client's behalf must provide written evidence that they represent the client.

i) A spouse, parent, adult child, or adult sibling may be assumed to be the client's representative unless there is evidence to the contrary. The client's relationship with the representative should be validated and recorded whenever possible.

ii) A legal instrument of representation, such as a power of attorney, is binding evidence of representation.

(1) If the client or representative agrees, a copy of the legal instrument should be kept on file. If the client or representative does not agree, a notation should be placed on file indicating that the legal instrument has been examined and accepted.

iii) In other cases, a letter of representation signed by the client is acceptable as evidence of representation.

(1) A copy of the letter of representation must be kept on the client's file for future reference.

2.5 ACCURACY AND CORRECTION OF PERSONAL INFORMATION

P27. Employees shall collect personal information directly from the client, using our intake form where the client has signed the form indicating that the information is accurate, complete and up to date.

P28. No matter how client information is collected, employees shall make every reasonable effort to ensure that the information collected is accurate, complete and up to date for its intended purpose.

P29. If the accuracy, completeness, or timeliness of personal information is in question, the client, or his or her representative, shall be contacted to verify the information and update it as necessary.

P30. Clients have the right to challenge the accuracy and completeness of the information about themselves and to have it amended as appropriate.

P31. Employees shall correct factual errors when notified of them by the client. In some cases employees may ask for verification, in which case correction will be dependent on verification.

P32. To change information that reflects a professional opinion or assessment, employees must advise the individual to make the request to the designated privacy contact person.

P33. If a challenge is not resolved to the satisfaction of a client, the substance of the unresolved challenge shall be recorded in the individual's record.

2.6 USE AND DISCLOSURE OF PERSONAL INFORMATION

P34. Personal information shall be used only for the purposes for which it was originally collected or for purposes that are clearly consistent with the original purpose.

P35. If personal information is to be used for a purpose that is not clearly consistent with the original purpose of collection, prior authorization from the employee's supervisor and subsequent client written consent are required.

P36. Personal information shall be treated as confidential and not disclosed to any person, other than the client, except as stated in the FOIP Act. [see "www.oipc.sk.ca"]

P37. The FOIP Act allows limited specified exceptions to use or disclose personal information without client consent.

P38. Employees must be familiar with our protocol(s) for sharing personal information with other service providers.

P39. In the event that we are compelled to produce personal information pursuant to any applicable legislation, regulation, or any order of any court, tribunal, administrative body or other authority with jurisdiction, the request must be referred to the designated privacy contact, who will consult with RODS and the program funders.

2.7 INFORMATION SECURITY

P40. We shall take all security measures reasonably necessary, including those set out in any instructions issued by our funders for the protection of personal information against unauthorized use or disclosure. Our security measures shall be appropriate for the sensitivity of the information being protected regardless of the format in which it is held.

P41. We shall make employees aware of the importance of maintaining the confidentiality of personal information.

P42. We shall restrict access to personal information to authorized personnel with a "need to know" and to other parties to whom disclosure is authorized under the law.

P43. We shall secure electronic files by user authentication and authorization measures, encryption, and/or other measures as appropriate.

P44. Electronic files containing personal information will not be stored or transported on portable computing devices (such as laptop computers, USB sticks, CD's, DVD's, smartphones, or tablets) unless they have been encrypted.

P45. Employees shall secure paper files using physical access controls such as locked filing cabinets, secure storage rooms and locked desks.

P46. We will restrict access to personal information to the premises. No personal information will be allowed to be copied or transferred to portable computing devices that leave our premises without the prior approval of a supervisor.

P47. Transmitting sensitive information by email, including but not limited to personal information about a client, requires the prior approval of a supervisor.

2.8 RECORDS MANAGEMENT

P48. We will keep all personal information transferred, collected, created, maintained, or stored securely.

P49. We will retain personal information only as long as is reasonable to fulfill the purposes for which the information was collected, or for legal or program purposes.

P50. Personal information that has been used to make a decision about an individual should be retained long enough to allow the individual access to the information after the decision has been made.

P51. Retention guidelines should include minimum and maximum retention periods.

P52. We shall apply appropriate security measures when destroying personal information, including shredding paper records and permanently deleting electronic records in accordance with applicable Funders records retention and disposition policies; and taking care to prevent unauthorized parties from gaining access to the information.

P53. A record of destruction will be kept to verify what client documents were destroyed and when.

2.9 PRIVACY/SECURITY BREACHES

P54. The Saskatchewan Information and Privacy Commissioner has prepared a reference document that presents privacy best practices for dealing with a privacy breach. The document is available at http://www.oipc.sk.ca/Resources/Helpful Tips - Privacy Breach Guidelines - September 2010.pdf. Our organization follows these best practices.

P55. Employees may become aware of a breach through a complaint from the public, from observing something occurring or through personal involvement with the incident. Regardless of how an employee becomes aware of a breach, any employee who

becomes aware of a real or suspected breach of privacy or security shall report the breach to his or her supervisor/manager immediately.

P56. It is crucial that the supervisor reports the incident to the designated privacy contact person, who will in turn consult with RODS Executive Director and the funders.

P57. Any real or suspected breach of privacy shall be investigated as soon as possible after the breach is known and involve the participation of the Funders.

P58. Affected individuals will be notified as appropriate, depending on the severity and circumstances of the breach. Individuals who could suffer harm from the breach will be notified as soon as possible.

P59. The investigation shall make the following findings:
- a) Whether a breach of privacy or security actually occurred.
- b) When the breach occurred.
- c) Why the breach occurred.
- d) How many persons were affected by the breach.
- e) The severity of the breach's effects on affected persons and whether they need to be notified.
- f) The measures required to prevent a reoccurrence of the breach and how such measures should be implemented.

P60. Measures to prevent a re-occurrence of any breach shall be recorded and incorporated into RODS policy and/or procedures as necessary.

P61. We will notify the program funder/s which can then inform the Office of the Saskatchewan Information and Privacy Commissioner if circumstances dictate.

2.10 ACCESS TO CLIENT INFORMATION

P62. We shall provide reasonable and timely access to clients who identify themselves and request access to view the information we have collected about them.

P63. If we receive a request for access from a third party or a formal request under the FOIP Act, for client records in our possession, employees must:
- a) advise the requester to make the request to the funder; and
- b) not disclose the information in the records unless otherwise directed in writing by Funders.

2.11 INFORMING CLIENTS AND THE PUBLIC

P64. We will provide a copy of this privacy policy document to anyone on request.

P65. We will post a copy of this privacy policy on our web site and make copies available in our office(s).

P66. We will display a brochure that explains the purpose and privacy implications of collecting client information. The brochure will be kept in a location visible to all clients for their easy access.

2.12 PRIVACY QUESTIONS AND COMPLAINTS

P67. If a client is not satisfied with the response they receive regarding an inquiry or complaint about our policies and practices relating to the handling of personal information, the employee shall direct the client to contact the designated privacy contact person.

P68. If a complaint is found to be justified, we shall take appropriate measures, including, if necessary, amending our privacy policy and practices.

P69. If the complaint concerns personal information under our Funders' possession or control, the privacy contact person must direct the complaint to the Funders' contract manager.

3 GUIDELINES

3.1 INFORMATION SECURITY

Information security means taking reasonable security measures to protect the personal information in the possession or control of RODS, from risks such as unauthorized access, collection, use, disclosure, copying, modification, disposal and destruction.

The guidelines in this section and the best practices in the following section are not strictly required by the privacy policy principles and statements. However, the guidelines and best practices provided here will provide good privacy-related information security for the appropriate balance between information security and ease-of-use.

Information security issues are subject to rapid change. We will review this information security at least annually and when new security issues become known, to address new and emerging security issues.

For more information about security, please see section 4.1 "Security Best Practices" in the APPENDICES.

3.1.1 ADMINISTRATIVE MEASURES

G1. The privacy contact person has been designated with overall responsibility for security within RODS.

G2. Information session for board members, employees and volunteers, to ensure they are aware of and understand their responsibilities including:
   a) security policy and practices,
   b) permitted access use and disclosure of personal information,
   c) retention and disposal policy,
   d) requirements for password maintenance and proper password security.

G3. Sanctions for breaches of the privacy policy and a process for reporting and investigating breaches.

G4. Limit access to personal information by following the "need to know" principle. Staff should only be provided file cabinet keys and passwords to access files they need to perform their duties. Review access rights periodically and remove access when no longer required by an employee.

G5. Check the references and background of each employee to ensure that he or she is a suitable person to have access to sensitive information, information systems and the facilities where they are located.

G6. Require employees to sign a confidentiality agreement that clearly defines individual responsibilities for security, including the protection of personal information.

3.1.2 PHYSICAL SAFEGUARDS

G7. Lock file cabinets and areas where files are stored when no one is there. Provide keys only to staff needing access to the files to perform their work.

G8. Establish a nightly closing protocol requiring employees to lock all office doors and cabinets; log out of all computers; remove all documents containing personal information from desks, fax machines and printers; and install intrusion alarms (where needed/or applicable).

G9. Shred or otherwise destroy paper files before disposing them.

G10. Securely wipe all personal information from hard drives before they are discarded, sold or donated.

G11. Store personal information on portable devices like laptops, flash drives and CDs or DVDs only when necessary; only store as much personal information as is necessary for the task and delete as soon as possible.

G12. Do not leave unattended, and securely lock away, portable media devices when not in use.

G13. Position computer monitors so that personal information displayed on them cannot be seen by unauthorized personnel or by visitors.

G14. Locate printers that are used by staff to print items containing personal information in a secure location.

G15. Gain required approval prior to taking records off-site.

3.1.3 TECHNOLOGICAL SAFEGUARDS

G16. Use software, hardware or operating system access controls such as passwords, termination on inactivity and clearance of display screens to limit access to files containing personal or otherwise sensitive information.

G17. Keep firewalls and anti-virus/anti-spyware software up-to-date, to protect against invasive malware.

G18. Password-protect portable media devices such as laptops and USB flash drives and encrypt to current encryption standards.

G19. Do not install software that has not been approved for use by your organization.

G20. Grant remote access into RODS internal office network only for individuals who need that access. Review access rights periodically and remove access when no longer required by an employee.

G21. Establish security controls for remote access to information systems.

G22. Where practical, erase the contents of fax machines and photocopiers prior to repair or disposal.

G23. Ensure that passwords are not easily guessed or compromised:
   a) Do not use any word or phrase that might be found in a dictionary.
   b) Make sure all passwords are at least eight characters long and include at least one upper case character, one number and one punctuation symbol. (Holding down the SHIFT key while creating and entering your password is a good idea; it creates passwords that are hard to guess.)
   c) Change passwords at least every 90 days and whenever there is a chance that they may have been compromised.
   d) NEVER share passwords, except those that have to be shared to exchange encrypted documents.

4 APPENDICES

4.1 SECURITY BEST PRACTICES

4.1.1 AT THE OFFICE

4.1.1.1 PERSONAL CONVERSATIONS

1) Do not discuss sensitive or personal information in areas where there is potential for conversations to be overheard.

2) Have regular interpreters/translators sign an oath of confidentiality. If it is not feasible to have an interpreter/translator sign an oath of confidentiality, such as in an emergency, be sure to advise them that everything they hear in the course of providing interpreter/translator services must be kept confidential.

4.1.1.2 SECURING PAPER RECORDS

3) Follow a “clean desk” policy. Do not leave confidential or sensitive files on your desk.

4) Place files in secured storage areas such as locked cabinets and desk drawers during lunch or other breaks away from your desk.

5) Do not store files in areas where the general public has access.

6) Files containing personal information or sensitive business information should be placed in locked offices or storage after business hours. Even though the office is secured, the premises are accessible by “outsiders” such as cleaning, security and maintenance staff.

7) Shred or otherwise destroy paper files before disposing them in accordance with your organization’s retention policy.

4.1.1.3 PROTECTING ELECTRONIC RECORDS

8) Computer monitor screens should not be visible to others.

9) Laptops used in high traffic areas should be cable-locked to reduce the possibility of theft.

10) Keep your portable devices out of sight when you are away from your work area for extended time periods and after business hours.

4.1.1.4 SAFEGUARDING THE OFFICE PREMISES

11) Ensure that there is reception coverage as long as the office door is open.

12) Unescorted visitors should not be allowed. Question unescorted visitors in your area – start with “May I help you?” Ask for identification if the person is unknown to you.

13) Ensure that the office door is locked after business hours. Alarms or detection systems, if installed, should be activated.

4.1.2 TRANSMITTING INFORMATION

4.1.2.1 TELEPHONE (CELL AND DESK PHONES)

14) Be aware that in public areas or open office, your conversation may be overheard by others. If conversations are sensitive, consider a using closed room.

15) Most phones have voice mail that records messages. These are retrievable through a code which should only be known only to you. Treat it like you would a password.

16) If you must leave a voice mail message, make sure it is for the right person and avoid leaving sensitive information. Be aware that family members or co-workers may have access to messages not intended to them.

17) Cell phones and smart phones may also contain text messages and contact lists which should be protected by password. Do not leave text messages that contain personal information on your cell phone/PDA (Personal Digital Assistant).

18) Consider the sensitivity of information in case of loss or replacement of a ‘smart’ phone. A lot of confidential information may also be contained in ‘smart’ phones.

19) Never communicate personal or confidential information when using a cell or cordless telephone. This type of communication can be easily intercepted.

4.1.2.2 WIRELESS DEVICES

20) Do not connect on a public internet (WIFI) or unsecured home network.

4.1.2.3 FAX

21) Do not leave unattended documents that are sent or received on the fax machine.

22) Pre-programmed fax numbers should be regularly checked to ensure accuracy. Take care when using distribution lists.

23) When sending sensitive or personal information, first contact the recipient to schedule the transmission so they can be at the receiving fax machine when the fax arrives, unless you know that the receiving machine is not accessible to unauthorized persons.

24) Fax documents should be sent under a fax cover sheet that contains sender information and a disclaimer similar to the following:

    This e-mail and any files transmitted with it are intended only for the named recipients and may contain legally privileged and/or confidential information. If you are not the intended recipient please do not disseminate, distribute or copy this e-mail without the consent of the sender.

25) Do not use internet services to send or receive faxes through e-mail or websites unless their use has been authorized within your organization.

4.1.2.4 E-MAIL

26) The organization should provide business e-mail addresses to all employees and employees should be informed that e-mail messages to and from those addresses are accessible to the management of the organization.

27) Only use the office email system to perform your day-to-day job duties. Using a personal email address for official purposes carries a number of security risks and should be avoided because information is stored on servers outside your organization's network and therefore outside its control.

28) Do not forward any unencrypted e-mail containing personal or otherwise sensitive information to an outside network, or create any automated process to do so. Sending unencrypted confidential information from the office to your home e-mail to work at home is to be avoided.

29) When choosing e-mail as a means of communication, be professional. Keep in mind that e-mail sent by you can be kept for a long time and can be used during an investigation. Your e-mail content may be available to a number of people such as computer personnel.

30) Do not transmit any e-mail message you would not want someone other than the intended recipient to see.

31) Do not transmit any personal information by e-mail unless you have the appropriate authority to do so, and you have confirmed the intended recipient.

32) Do not share your e-mail password with anyone. If you must have a co-worker have access to your e-mail or files (e.g. during vacation) use delegated authority if your e-mail system has this feature. Delegation allows a co-worker or manager to use their own user ID and password to read or send e-mails on your behalf.

33) If you use a distribution list, verify that the list is up-to-date and that the recipients for a particular message are authorized to receive the message before sending it to the entire list.

34) If you must send sensitive information by e-mail, safeguard information by e-mailing it in an encrypted attachment and phoning the person to provide the password to use to decrypt the attachment. (Note that additional software may be required for the encryption and decryption of attachments, depending on which software you used to create the attachment. For example, recent versions of Microsoft Word will encrypt documents, but other word processors may not.)

35) Emails sent outside the office network should carry a disclaimer similar to the following:

"This communication may contain information that is privileged or confidential and is intended for the use of the intended recipient only. If you are not the intended recipient, you

should not use, copy or take any action in reliance on it. If you have received it in error, please notify the sender at once and permanently all copies in your possession".

36) Do not open unknown or unsolicited attachments. They may contain viruses or spyware.

4.1.3 AWAY FROM THE OFFICE

4.1.3.1 TAKING RECORDS OUT OF THE OFFICE

37) Avoid using information off-site unless absolutely necessary.

38) Permission from your supervisor or manager is required before you take any records out of the office.

39) Only take the information you need, not the whole file.

40) Leave a list at the office of what you take off-site.

41) It is highly recommended that laptop hard drives use whole disk encryption systems (e.g. TrueCrypt) while USB sticks MUST use software encryption (e.g. TrueCrypt) or hardware encryption (e.g. IronKey).

4.1.3.2 TRANSPORTING RECORDS

42) Transport hard copy information in containers (e.g., briefcases, envelopes), not loose.

43) Keep sensitive files with you at all times. Never leave files unattended in your car.

44) If you must leave files in your car, store them in a briefcase in the trunk (out of sight). Put them in the trunk *before* you depart, not after you've parked at your destination.

45) If you must leave your laptop and other equipment in a vehicle, put them in the trunk, before you depart.

46) Never leave your laptop, or any other equipment that stores information, unattended, even for a moment. If you must take it on public transportation, it *must* be in your carry-on luggage, which *must* be kept in your possession at all times.

4.1.3.3 ACCESSING WORK INFORMATION SYSTEMS WHILE AWAY FROM THE OFFICE

47) If you have to get into the internal office network to do your job away from the office, request a RODS remote access setup.

4.1.3.4 DISCUSSING SENSITIVE OR PERSONAL INFORMATION IN PUBLIC PLACES

48) Work in a private area where the public will not see paper files or hear sensitive or personal information during phone conversations.

4.1.3.5 REDUCING THE RISK OF A PRIVACY OR SECURITY BREACH AT HOME

49) Do not use your home or public computer to process sensitive information. Always use a work-issued device.

50) A direct wired connection is the preferred option to a wireless connection when connecting to the office network from home.

51) If you are using a wireless connection, the connection must be secured with network password containing at least 8 characters. Wireless connections must be encrypted using the WPA (Wi-Fi Protected Access) standard or better. Note that WEP (Wired Equivalent Privacy) encryption is easily broken. Wireless connections within the office *must* be encrypted. Consult your computer services provider for help or more information about wireless network encryption.

52) Keep information secure and away from household members or visitors.