Digital Communication Tip Sheet

Community and Social Services (CSS) Programs: Income and Employment, AISH, PDD, FSCD and Alberta Supports

Overview

Technology is widely used by CSS program staff to connect with individuals and service providers. Staff must understand the communication options available, how to use each effectively and how to document the communication while also protecting privacy.

Communication Method and Information Security

Discuss communication options and preferences with individuals early on to establish processes. Although an individual may prefer to communicate using a particular method, staff may decide a method more appropriate to the circumstances.

Taking reasonable steps to protect the personal information of individuals and families is extremely important. This means that all employees are responsible to ensure that reasonable security measures are in place based on the sensitivity of the information. CSS uses multiple applications to store information and each application has a unique security classification. Therefore, the rules for storing and transmitting information could vary. Some information is classified as 'protected' whereas other information is classified as 'public' (i.e. program applications and forms). For more information, please refer to The Technical Guide: Transmitting Data and Information. The document Safeguarding Government Information is also a valuable resource.

For the purposes of programs and services under Alberta Supports, any time staff are collecting information from an individual using any communication method they should be providing the Common Notification. Please refer to the document Understanding Common Notification for Programs and Services under Alberta Supports for further information.

Any communication regarding program decisions must be made following current program policy.

Communication Method	Description	Information Security Safeguards
All	• Refer to the GOA Social Media – Web 2.0 Policy	• Only send communications from Government of Alberta (GOA) devices and your GOA account. Report any lost/missing devices. • Ensure you are using the correct email address, phone/fax number or meeting ID's. • Ensure communication does not identify the person receiving services and does not disclose individual information. • Any "gov.ab.ca" email messages and all internet activity from a government computer or address can be tracked and will be attributed to the GoA and an individual user. The GoA has the right to investigate and monitor the use of its equipment and systems as warranted.

Email	• Email is a preferred method of communication for many individuals.
	• It can be useful to get updates and exchange a variety of information, such as sending and receiving documents.
	• For more information, reference the Protecting Emails and Electronic Documents Information Sheet and the Use of Government of Alberta **Internet** and E-mail.
	• Voicemail messages received on VOIP phones send an email with the voicemail message. Refer to Managing Voicemail as Official Records in a Unified Communications (UC Environment).
		• When sending documents to internal GoA emails, you are not required to password protect the document.
		• When sending confidential, identifying or sensitive information external to the GoA, use one of the following two methods:
		  • Secure, encrypted website https://sendfile.alberta.ca. For more information, access the Enhanced File Transfers information. Individuals have the ability to upload a document in return.
		  • Password protected document. Where possible, send documents in PDF and locked format so recipient cannot make changes. Send password separately (not in the same email).
		• Do not provide identifying information in the email subject line; keep information in the body of the email as generic as possible.
		• Utilize options in existing Information Technology (IT) systems for communication (i.e. form letters, Team Collaboration in Mobius) instead of email.

Communication Method	Description	Information Security Safeguards
Text Messages	• Access to free applications and Wi-Fi hotspots means text messaging can be a convenient way to communicate. • Text can be useful when communicating about changed appointment locations/times or requesting an individual contact their worker. • If text messaging is the preferred method of contact, it is important for staff to set up clear boundaries on when they will respond to messages.	• Only text from a GoA device. • Keep text conversations to general information (no personal information or CSS decisions) • Use other means of communication if no response is received, such as phone or face-to-face. • If using a text message application from a computer, search the name of the application on the GoA certified software list and only use an application that is on this list.
Fax	• Staff may receive or send information by fax for individuals that may not have access to other forms of technology, or is their preferred method of communication.	• Send a confirmation fax before sending confidential information. • Send separate faxes when needing to provide information about multiple individuals. • If faxing an individual at a public fax machine (i.e. library), ensure the individual is waiting to receive the fax so that others do not pick up the information.
Video Conferencing / Conference Call	• Conferencing helps facilitate communication with multiple parties in a variety of locations e.g. inter-regional/provincial case discussions, obtaining medical professional updates/recommendations when in-person attendance is limited.	• Use a private workspace with a closed door. • Conduct introductions at the beginning of the meeting. • When audio or video recording, ensure consent is gathered.
Skype / Lync	• Skype/Lync is frequently used for internal GoA communications. Refer to the Using Skype Safely document for some tips. • For more information on managing Skype messages, please follow the directions in Managing Instant Messages.	• Skype can be used externally with clients and service providers.

Communication Method	Description	Information Security Safeguards
Social Media	• Social media includes applications such as Facebook, Instagram, Twitter, Snapchat, etc.	• Do not use any social media application or platform for communication because GoA loses custody of the information as soon as it is on social media
Cloud Storage	• Information that is maintained, managed and stored remotely • Examples include google docs, dropbox, etc.	• The use of Cloud Storage is not supported for sharing documents • The Data Security in the Cloud document has updated information on cloud storage policy

While some technologies are less formal, consider the Code of Conduct and Ethics for the Public Service of Alberta in all communications, both offline and online (i.e. remain impartial, disclose conflicts of interest and maintain/respect confidentiality and privacy).

Identity Verification

It is important to ensure you are communicating and sharing information with the correct individual. If you are communicating with someone you don't know and need to verify who they are, use two channels of communication (email, phone, face-to-face, fax, etc.). Some examples of best practices include:

1. Email/text the individual for the first time while in a face-to-face/phone conversation to ensure that they are receiving the email/text.
2. Have the individual verbally confirm 3 pieces of identifying information available on the file (Social Insurance Number, birth date, address, Alberta Health Care number, etc.)
3. If your IT system allows, create a security question and response

When unclear about who you are communicating with, do not send identifying information by email/text/fax, etc.

Documentation

Document all communication. Inform individuals that communications are documented regardless of the technology used. Capture all communication in accordance with existing program standards in relevant systems such as Mobius, TOI, CSS or FSCDIS.

Technology Type	Documentation Requirements
All	• In the contact note, specify the method of communication used and summarize the information • Print and file (or image) any documents or attachments provided
Emails	• Once documented, email messages need to be kept for a period of one year and then can be deleted

For more information on information management of documentation, refer to Enterprise Information Management's Official and Transitory: A Guide for Government of Alberta Employees.

Additional Resources

There are a number of mandatory Government of Alberta (GoA) courses accessible in Noverant (https://goa.noverant.com/fcf/protected/) related to the collection, use and storage of information:

Information Management	Module 1 – What is Information Management Module 2 – How to Manage Information Module 3 – Risks and Benefits of Information Management
Emails	Module 1 – Introduction to the FOIP Act and Access to Information Module 2 – Protection of Privacy
Cyber Security www.security.gov.ab.ca	• Malware and Ransomware • Phishing and Social Engineering • Policies, Security and Reporting Incidents • Protecting Information When Working Offsite • Safe Electronic and Physical Document Handling • Secure Passwords