DRAFT SAMPLE INTERNAL GUIDELINES

ACCEPTABLE USE GUIDELINES – Cell/smartphones

Drafted (date)
Approved by:
Effective: (date)
Last review: (date)
Next review by: (date)

These guidelines are internal to program staff. These guidelines are intended to be complimentary and supplementary to the [your organization] "Computer/Network/Internet/Electronic Mail/Office and Mobile Phone Usage Policy". This is a living document that will be updated as the situation changes. Staff are encouraged to contribute to its ongoing development.

Staff are provided with smart phones in order to provide service to clients using communication platforms that are only accessible via smart phone. Staff should note that there will be no expectation of personal privacy on an assigned cell phone, as all information can be accessed by management at any time.

Each full-time staff will have an individual phone/phone number assigned to them. Part-time staff will share an assigned phone between them.

GENERAL USAGE

Staff will use assigned smart phones for work-related purposes only. Staff are not to conduct personal business using [your organization] smart phones. This includes but is not limited to sending/receiving personal messages through text or other communication platforms, making/receiving personal phone calls, downloading apps for personal use (other than with the intention of enhancing personal accessibility) and accessing personal social media accounts using the [your organization] phone.

[your organization] staff are prohibited from using their assigned smart phone for any purpose, hands on or hands-free, while driving or operating a vehicle.

Secure wifi or cellular data only should be used when using [your organization] smart phones. Public networks (including networks within the [your organization] that are not password protected) should not be accessed using [your organization] smart phones.

Personal friend requests on social media – Requests from clients to connect with [your organization] staff can be accepted at the discretion of the individual staff.

PHYSICAL HARDWARE

Each assigned smart phone includes a charger, headphones, headphone adaptor, and a case. Staff are responsible for the care and maintenance of each of these items and should immediately inform their supervisor if there are any issues with the phone itself or any of the physical hardware included. A case by case decision will be made in terms of reimbursement for the repair or replacement cost of a damaged, lost or stolen smart phone or hardware accessory if its damage, loss or theft was due to staff negligence.

Smart phones are to be kept in a locked drawer in the [your organization] office when not in use. Staff may take their assigned phone off-site only in the event that they require the phone for a client meeting that is taking place outside of office hours and the Staff has permission from their supervisor to bring the phone off-site. Staff should notify their supervisor by e-mail in advance that they intend to take the phone off-site so that there is a written record of the phone's whereabouts.

PRIVACY SETTINGS

Individual Staff may choose to adjust the settings of their assigned smart phone to suit their usage preferences. Certain settings must remain unchanged for privacy purposes:

- Smart phones should be protected by a passcode. Passcodes should be known only to the Staff assigned to the phone and the [assigned manager or Director in your organization]. The [assigned manager or Director in your organization] must be informed of any changes to the passcode.
- Fingerprint access should not be activated, with the exception of staff for whom this option enhances accessibility

Passcodes must be changed every 3 months. The [assigned manager or Director in your organization] must be informed immediately of an update to an assigned smart phone's passcode.

PHONE USAGE

[your organization] assigned smart phones include the following voice and data plan:

Sample Voice & Data Plan

Plan Cost /Feature Options	**Voice and Data - 1**
Included Anytime Minutes -	Unlimited Local
Additional Local Minute Rate (per min)	N/A
2500 minutes of Call Forwarding	Included, LD charges may apply
Call and name display	Included
Group Calling	Included

Call Waiting	Included
6 way conference calling	Included
Voicemail	Included
Call Display	Included
Unlimited local Incoming calls	Included
Unlimited SMS & MMS - Canada	Unlimited
Per minute Rate	$0.10/min and $0.20/min
Blackberry 10 /Smartphone	1 GB Canada
Data Pooling	Included for domestic
Fixed pay per use rate - Voice	$0.25/Min
Fixed pay per user rate - Data	$1.00/MB

As such, the following best practices for phone usage are in place:

- Voice calls should only be made to or answered from known local numbers
    - If an incoming call is from an unknown number, do not answer
- Text messages (SMS/MMS) should only be sent to and received from Canadian phone numbers
- Whenever possible, the smart phone should be connected to WiFi rather than using data

When requested, Staff will review monthly smart phone billings with supervisors, verifying the accuracy of the billing, and identifying any charges that are outside of what is included in normal monthly billing (listed above).

In the event that in extenuating circumstances additional charges are incurred (ex. answering a long-distance phone call from a client), this should be noted in client case notes and [assigned manager or Director in your organization] should be notified by e-mail ASAP.

SOFTWARE/APPLICATION UPDATES AND DOWNLOADS

Staff may be prompted to download updates to their assigned smart phone as well as for individual applications. As these updates may include changes to privacy policies or terms and conditions of usage, Staff should consult with the [your organization] Director prior to downloading any updates.

Applications in addition to those that are listed in Appendix A should not be downloaded to [your organization] assigned smart phones. If staff would like to download additional

applications they must make a request to the [assigned manager or Director in your organization].

APP USAGE

Text for sample apps that might be common to a settlement organization (in this case, assumes us of iPhone):

WhatsApp
Each [your organization] smart phone has an individual WhatsApp account. [your organization] Staff are to use this account to communicate with clients who prefer to access service through WhatsApp. Staff may prefer to use the app through the phone itself or through the desktop application.

[your organization] Staff must communicate with clients using only the WhatsApp account associated with their assigned phone number. This phone number should appear in each Staff's e-mail signature.

All interactions on WhatsApp are end-to-end encrypted (https://www.whatsapp.com/security/). As such WhatsApp is a preferred method of communication and document-sharing between Staff and clients. Staff should verify that end to end encryption is activated by looking for the indicator in "contact info" or "group info" during their communications with clients.

In order to ensure that privacy is respected, backup data to iCloud for the WhatsApp app should be turned off in the settings of the smart phone (Settings > General > Storage & iCloud Usage > Manage Storage > Backups).

Facebook and Facebook Messenger
[your organization] Staff can access Facebook and Facebook Messenger through their assigned smart phone or on their desktops. Staff must have a professional account that is separate from their personal account to be used for communication with clients and for other [your organization] communications. Professional account information including login and password must be shared with the [assigned manager or Director in your organization]. Professional Facebook accounts will be transferred over to the incoming Staff in the event that a [your organization] Staff leaves their position.

Facebook Messenger conversations between Staff and clients must be in "secret" mode to ensure end-to-end encryption. To learn how to set up secret conversations, visit this link: https://www.facebook.com/help/messenger-app/iphone/811527538946901?rdrhc.

Both Staff and clients need to be in "secret" mode in order to ensure that encryption is in place.
As end-to-end encryption for Facebook messenger is only currently available through the Messenger app for iOS and not through desktop, Staff should only communicate with clients via Facebook Messenger using the app on their assigned smart phones.

Communication with clients using Facebook for desktop (user-to-user messages or other methods of communication through the platform) or Messenger.com for desktop is not secure. Staff should take every reasonable measure to ensure that clients are aware that they are not communicating through a secure channel and to remind clients not to share personal information through these means.

Viber
Each [your organization] smart phone has an individual Viber account. [your organization] Staff are to use this account to communicate with clients who prefer to access service through Viber. Staff may prefer to use the app through the phone itself or through the desktop application.

[your organization] Staff must communicate with clients using only the Viber account associated with their assigned phone number. This phone number should appear in each Staff's e-mail signature.
All interactions on Viber are end-to-end encrypted (https://www.viber.com/en/privacypolicy). As such Viber is a preferred method of communication and document-sharing between Staff and clients.

In order to ensure that privacy is respected, backup data to iCloud for the Viber app should be turned off in the settings of the smart phone (Settings > General > Storage & iCloud Usage > Manage Storage > Backups).

Skype
[your organization] Staff can access Skype through their assigned smart phone or desktop. Staff should have a professional Skype account that is separate from their personal account to be used for communication with clients and other [your organization] communications. Professional account information including login and password must be shared with the [assigned manager or Director in your organization]. Professional Skype accounts will be transferred over to the incoming Staff in the event that a [your organization] Staff leaves their position.

Skype does not offer end-to-end encryption and therefore is not a completely secure method of communication (https://support.skype.com/en/faq/FA31/does-skype-use-encryption). Staff should take every reasonable measure to ensure that clients are aware that they are not communicating through an entirely secure channel and to remind clients not to share personal information through these means, particularly when it is not a Skype-to-Skype interaction.

FaceTime and iMessage
Staff can communicate with clients who use Apple products through FaceTime or iMessage using their assigned smart phone. Staff should verify that text messages being sent or received from clients are iMessages and <u>not</u> text messages (MMS/SMS), and that voice/video calls are FaceTime calls and <u>not</u> regular voice calls.

All interactions through FaceTime and iMessage are end-to-end encrypted (https://www.apple.com/ca/privacy/approach-to-privacy/). As such FaceTime and iMessage are preferred methods of communication between Staff and clients.

E-mail
Personal e-mail accounts should not be linked to assigned smart phones. For security reasons, @ymcaywca.ca e-mail accounts should not be linked to assigned smart phones.

E-mails sent and received through Staff's @ymcaywca.ca addresses are not encrypted and therefore e-mail is not a completely secure method of communication. Staff should take every reasonable measure to ensure that clients are aware that they are not communicating through an entirely secure channel and to remind clients not to share personal information through e-mail.

Staff should refer to [your organization] "Computer/Network/Internet/Electronic Mail/Office and Mobile Phone Usage Policy" for acceptable use of e-mail.

GoToMeeting
Due to the fact that accounts are shared within the [your organization] team and Y staff, it is not recommended to access GoToMeeting through a smart phone application.

LinkedIn
As LinkedIn does not provide any kind of secure messaging option it is not recommended to communicate with clients through this platform. [your organization] staff should not send invitations to clients to connect through LinkedIn; if a client sends a request to connect to a [your organization] staff member it is up to their discretion whether or not they choose to accept.

SOCIAL MEDIA USAGE

[your organization] staff are reminded that with each social media post or comment, internet site visit and e-mail transmitted, the [your organization] is being represented. Usage and messages must be accurate, appropriate, respectful, and must not subject the [your organization] to potential liability. For [your organization] employees who use their own personal social media profiles or accounts to post information about the [your organization] (including through LinkedIn) a clear statement to the effect that 'these views are solely your own' should be included in your profile information.

IN CASE OF LOST OR STOLEN DEVICE

Staff should inform the [assigned manager or Director in your organization] immediately if their device is lost or stolen. The [assigned manager or Director in your organization] will inform the [your organization] IT department to ensure that data is remotely wiped from the device and that the phone plan is discontinued.

DOWNLOADING DOCUMENTS/PHOTOS

Documents or photos sent by clients containing sensitive or personal information through applications accessed through assigned smart phones must be deleted as soon as they are no longer needed by the Staff. Smart phones must not serve as document storage.

CLIENT SERVICE GUIDELINES

All communication between Staff and clients must be tracked in CATS or alternative case note methods. Text communication (including written communication through any and all channels listed above) between Staff and clients must be copied and pasted in to CATS case notes or saved in the client's digital folder on the shared drive to ensure that a record of conversation is kept by the [your organization].

Appendix A: Approved mobile applications

1. WhatsApp
2. Viber
3. Facebook
4. Messenger
5. Skype
6. iMessage
7. FaceTime