Safety & Privacy Recommendations for Online Communication

Build ON delivers pre-arrival service via various online communication platforms for the convenience of our clients. The YMCA-YWCA of the National Capital Region takes our commitment to privacy and the online safety of our clients seriously. As a client accessing online pre-arrival services, it is your responsibility to understand the safety and privacy implications of available communication methods in order to make informed decisions about how you share information online.

This document outlines the security level of each communication method according to the most updated privacy policy of each platform. Please review this document before choosing your preferred method of communicating with Build ON. The number of gold stars reflects the relative level of security. You are encouraged to contact Build ON staff if you have any concerns or questions.

 **WhatsApp** 

All interactions on WhatsApp are end-to-end encrypted. That means that only communicating users can read messages and access shared documents. As such, WhatsApp is a preferred method of communication and document-sharing. For more information, read WhatsApp's security policy terms here.

 **Viber** 

All interactions on Viber are end-to-end encrypted. That means that only communicating users can read messages and access shared documents. As such, Viber is a preferred method of communication and document-sharing. For more information, read Viber's privacy policy terms here.

 **FaceTime and iMessage** 

All interactions through FaceTime and iMessage are end-to-end encrypted. That means that only communicating users can read messages and access shared documents. As such, FaceTime and iMessage are preferred methods of communication. For more information, read Apple's privacy policy terms here.

 **Skype** 

Skype does not offer end-to-end encryption and therefore is not a completely secure method of communication. You should not share personal information or documents that you wish to remain secure via Skype particularly when it is not a Skype-to-Skype interaction. For more information, read about Skype's use of encryption here.

 **Facebook Messenger** 

End-to-end encryption for Facebook messenger is only currently available through the Messenger app for iOS and Android. That means that Facebook for desktop and Messenger.com for desktop are not secure and you should not share personal information or documents that you wish to remain secure through these means. If you decide to use Facebook Messenger on your smart phone to communicate

with Build ON, we recommend that you ensure that conversations are in “secret” mode to activate end-to-end encryption. To learn how to set up secret conversations, visit this link.

 **E-mail** 

E-mails sent to and from Build ON are not encrypted and therefore e-mail is not a secure method of communication. As such, you should not share personal information or documents that you wish to remain secure via these means.