**ChatWorld**

**What happens to your messages**

OK, this is nothing serious. We just need to talk with users about what happens to their messages.

**What happens to my messages? And are they encrypted?**

Yes, in transit, your messages are encrypted using SSL. However we do not recommend sending personal messages as once your message is transferred to the server, we do not know what happens.

**This is because our app uses a default Redis server hosted by MIT due to the fact that the ChatWorld app was developed in MIT App Inventor.**

**So is it safe to send *any* messages?**

Of course! Sending a general message such as “Hey there! The soccer match today is really cool!”, is OK. Because it is not at all personal. Even for custom builds, we do not provide extra encryption other than the SSL encryption used in transit.

**How safe really is it?**

SSL encryption is high-quality, meaning that:

1. Your messages will ONLY be transferred to the server, as SSL encryption verifies who it is sending it to, preventing man-in-the-middle attacks, A.K.A, a bad actor posing as the server.
2. SSL includes mechanisms that detect whether or not the data has been altered in transit, preventing against tampering.
3. The data is, again, encrypted, so it is not intelligible by a human.

However the app does not and isn’t planned to be able to provide E2E encryption. (end-to-end encryption), which is the highest level of protection available anywhere, which means that the data sent will always be encrypted, even once it has reached the server.

**I couldn’t understand much.**

In a nutshell, ChatWorld makes your messages into unintelligible gibberish until it reaches the server, where they are stored. Soon, we will make it so that you can send AND delete your messages at will.

In an even smaller nutshell, ChatWorld is safe, **but not to the highest standards.**

We still care about your messages, but,

**Don’t send personal messages on ChatWorld! Even with a custom build!**

**AND**

**Don’t download versions of the app that are from third-parties!**

**They could be infected with malware, disable encryption, or collect messages and share them with bad actors.**

That is all! Goodbye!