Acceptable Use Policy (AUP) - V21.1

1. About this Acceptable Use Policy

1.1 This Acceptable Use Policy (**AUP**) applies to Software supplied by ReadyTech Group companies (each, a **Company**), where this AUP is incorporated into contracts entered into by them with their customers.

1.2 This AUP outlines acceptable behaviours expected of any person using and/or accessing the Company's Software (**End Users** or **you**).

1.3 End Users must comply with this AUP and must not encourage, promote, facilitate, or instruct other End Users to breach this AUP.

1.4 End Users must act appropriately in all respects and must not display, store, distribute, transmit or otherwise make available communications or content using the Software that contains abusive, offensive, harmful or objectionable language, that has the potential to defame or libel others, or that infringes on the privacy rights or other rights of others. End Users must not view, download, copy, send, post or access information that is illegal, fraudulent or obscene when using or accessing any Software and must not use it in any way prohibited by this AUP or which would otherwise cause the Company loss and/or damage and/or negatively affect the Company's reputation, associated goodwill or cause the Company to fall into disrepute or dispute with any third party including its service providers.

2. End User prohibitions

2.1 Without limiting the above provisions of this AUP, in the course of any End User using and/or accessing any Software of the Company, the following are strictly prohibited:

(a) accessing any other person's account other than your allocated account;
(b) uploading any content about a person without the person's consent or using the Software to violate all or any legal rights of any person or company or other entity in any jurisdiction;
(c) using the Software (including by any intentional access, creation, modification, transmission, distribution or storage of information, data or material) in breach of the *Privacy Act 1988* (Cth) or any other applicable data protection laws in any relevant jurisdiction;
(d) using the Software in relation to crimes such as theft and fraud;
(e) using the Software in breach of any laws, including but not limited to, laws relating to the protection of copyright, trade secrets, patents or other intellectual property and laws relating to spam or privacy;
(f) unauthorised copying of copyrighted material including, but not limited to, the installation of any copyrighted software for which you do not have an active licence;
(g) using the Software in connection with the provision of negligent or unlawful services;
(h) exporting software, technical information, encryption software or technology, in violation of domestic and international export control laws;
(i) any form of computer hacking or introduction of malicious programs into the Company's or any of its service provider's networks, computers or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, broadcast attacks or any other flooding techniques) or otherwise violating the security or integrity of any network, computer or communications system or software application of the Company or its service providers;
(j) revealing your account password to others or allowing use of the Software by others who are not authorised to do so including by attempting to probe, scan or test the vulnerability of an account or the Company's Software;
(k) using the Software to actively engage in conduct that would make a person feel offended, humiliated harassed or intimidated or procuring or transmitting material that is in violation of sexual harassment or workplace relations laws;
(l) using the Software to offer or distribute fraudulent goods or services;
(m) using the Software to upload, store, display, transmit content that is invasive, defamatory, obscene and/or invasive including content that constitutes pornography, relates to bestiality, or depicts non-consensual sexual acts of any kind;
(n) using the Software to enact security breaches or disruptions of network communication is strictly prohibited. Security breaches include, but are not limited to, accessing data of which you are not intended recipient, logging into a server or account that you are not expressly authorized to access or corrupting any data, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
(o) using the Software to execute any form of network monitoring or crawling which will intercept data not intended for you without permission;
(p) using the Software to circumvent user authentication or security of any of the Company's hosts, networks or accounts or those of its customers or suppliers;
(q) using the Software to interfere with or deny service to anyone;
(r) using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, any persons' use of the Software;
(s) sending unsolicited email messages through or to users of the Software in breach of the *Spam Act 2003* (Cth);
(t) using the Software to send any form of harassment via email, or any other form of messaging, whether through language, frequency, or size of messages;
(u) using the Software to send email to any email address, with the intent to spam or harass;
(v) operating network services like open proxies, open mail relays, or open recursive domain name servers;
(w) using the Software to create or forward "chain letters", "Ponzi" or other "pyramid" schemes of any type; and
(x) use of the Software in breach of any person's privacy (such as identity theft or "phishing").

2.2 To the extent that this AUP does not include all of the provisions of the Amazon Web Services Acceptable Use Policy https://aws.amazon.com/aup/, those provisions are hereby incorporated into this AUP by reference.