Use Restrictions

> *Last updated: March 4, 2021*

We also recognize that however good the maker's intentions, technology can amplify the ability to cause great harm. That's why we've established this policy. We feel an ethical obligation to counter such harm: both in terms of dealing with instances where Screendesk is used (and abused) to further such harm, and to state unequivocally that the products we make at Screendesk are not safe havens for people who wish to commit such harm. If you have an account with any of our products, you can't use them for any of the restricted purposes listed below. If we find out you are, we will take action.

Restricted purposes

- **Violence, or threats thereof**: If an activity qualifies as violent crime in the United States or where you live, you may not use Screendesk products to plan, perpetrate, or threaten that activity.
- **Child exploitation, sexualization, or abuse**: We don't tolerate any activities that create, disseminate, or otherwise cause child abuse. Keep away and stop. Just stop.
- **Hate speech**: You cannot use our products to advocate for the extermination, domination, or oppression of people.
- **Harassment**: Intimidating or targeting people or groups through repeated communication, including using racial slurs or dehumanizing language, is not welcome at Screendesk.
- **Doxing**: If you are using Screendesk products to share other peoples' private personal information for the purposes of harassment, we don't want anything to do with you.
- **Malware or spyware**: Code for good, not evil. If you are using our products to make or distribute anything that qualifies as malware or spyware — including remote user surveillance — begone.
- **Phishing or otherwise attempting fraud**: It is not okay to lie about who you are or who you affiliate with to steal from, extort, or otherwise harm others.
- **Spamming**: No one wants unsolicited commercial emails. We don't tolerate folks (including their bots) using Screendesk products for spamming purposes. If your emails don't pass muster with CAN-SPAM or any other anti-spam law, it's not allowed.
- **Cybersquatting**: We don't like username extortionists. If you purchase a Screendesk product account in someone else's name and then try to sell that account to them, you are cybersquatting. Cybersquatting accounts are subject to immediate cancellation.
- **Infringing on intellectual property**: You can't use Screendesk products to make or disseminate work that uses the intellectual property of others beyond the bounds of fair use.

While our use restrictions are comprehensive, they can't be exhaustive — it's possible an offense could defy categorization, present for the first time, or illuminate a moral quandary we hadn't yet considered. That said, we hope the overarching spirit is clear: Screendesk is not to be harnessed for harm, whether mental, physical, personal or civic. Different points of view — philosophical, religious,

and political — are welcome, but ideologies like white nationalism, or hate-fueled movements anchored by oppression, violence, abuse, extermination, or domination of one group over another, will not be accepted here.

How to report abuse

For cases of suspected malware, spyware, phishing, spamming, and cybersquatting, please alert us at support@screendesk.io.

For all other cases, please let us know by emailing support@screendesk.io. If you're not 100% sure if something rises to the level of our use restrictions policy, report it anyway.

Please share as much as you are comfortable with about the account, the content or behavior you are reporting, and how you found it. Sending us a URL or screenshots is super helpful. If you need a secure file transfer, let us know and we will send you a link. We will not disclose your identity to anyone associated with the reported account.

Someone on our team will respond within one business day to let you know we've begun investigating.

**This policy and process applies to any product created and owned by Screendesk.*