

Smartsheet Inc.
Acceptable Use Policy

Last Updated: July 31, 2017

This Acceptable Use Policy (“**AUP**”) governs your use of Smartsheet’s website (www.smartsheet.com), our mobile applications, and the Smartsheet work collaboration platform (“**Platform**”). We will refer to these collectively as the “**Sites**”. When we refer to “**Services**”, we mean the Sites and the services available through them. Smartsheet reserves the right to modify or update this policy from time to time.

You agree not to use the Services in any way that could harm or impair others’ use; prohibited actions include:

- Breaching or otherwise bypassing any security or authentication measures.
- Transmitting viruses, malware, or any other malicious or destructive code. Prohibited items include: any routine, device, or other undisclosed feature (e.g. so-called time bomb, virus, software lock, drop dead device, malicious logic, worm, Trojan horse, or trap, back door or software routine) that is either (1) designed to delete, disable, deactivate, interfere with, or otherwise harm any software, program, data, device, system, or service; or (2) intended to provide unauthorized access or to produce unauthorized modifications.
- Distributing content that harms or interferes with the operation of any Smartsheet or third-party networks, servers, or other infrastructure.
- Using any robot, spider, data scraping or extraction tool, or similar mechanism.
- Using the Subscription Service for phishing scams.
- Accessing, tampering with, or using nonpublic areas within the Services or shared areas within the Services to which you have not been invited.

You agree that you will not, and will not permit others, to use the Services to:

- Commit or encourage fraudulent or illegal activities in violation of any applicable laws, rules, or regulations (including those related to child pornography, gambling, or piracy).
- Use, store, share, host, copy, distribute, display, publish, transmit, or send objectionable content; prohibited content includes content that is or could be deemed: offensive, inflammatory, hateful, defamatory, discriminatory, obscene, abusive, invasive of privacy, or harmful to others.
- Distribute unwanted, unsolicited, or harassing mass e-mail or send unwanted promotional or commercial content (“Spam”).
- Infringe or misappropriate any Smartsheet or third-party copyright, trademark, or other intellectual property, proprietary right, license right, or legal content protection.
- Mislead or confuse others by pretending to be someone else or pretending to represent an organization you do not represent.
- Distribute others’ personal and confidential information (e.g. credit card numbers, confidential national ID numbers, or account passwords) without their permission.

HIPAA

Under Health Information Portability and Accountability Act, certain information about a person’s health or health care services is classified as Protected Health Information (PHI). Unless you have signed a Business Associate Agreement with Smartsheet, you may not store PHI in Smartsheet. HIPAA compliance is dependent on your adherence to the Smartsheet HIPAA Implementation Guide. The guide provides information on features and security controls that must be adjusted to ensure HIPAA-compliance.

If you are interested in learning more about Smartsheet and meeting HIPAA obligations, please visit the [Contact Us Healthcare page](#). And a member of the team will follow up with you.

Reporting Potential Issues

If you encounter content that you believe violates the above policies, please report it to us using the “[Report Abuse](#)” link. Smartsheet reserves the right, but does not assume the obligation, to investigate any violation of this AUP or misuse of the Service.