

**Sift Acceptable Use Policy**  
**Last Updated: February 26, 2019**

In connection with your use of our services, in addition to your obligations under your agreement with Sift (the "Agreement"), you agree that you will not engage in any of the activities below nor permit or encourage any third party to do so. This policy may change as Sift grows, so please check back regularly for updates and changes. Capitalized terms used below but not defined in this policy have the meanings set forth in the Agreement. You will not:

1. knowingly or intentionally fail to implement the Software properly;
2. knowingly submit any information to the Sift Services that is false, incomplete, out-of-date, or misleading;
3. submit any sensitive personal information, such as full credit or debit card numbers, financial account information, full government identification numbers, account passwords, health-related information, information related to children under 16) or any other information that deemed "sensitive" or falling under "special categories" under applicable laws, rules or regulations;
4. circumvent any access or use restrictions, data encryption, or content protection related to the Sift Services, including accessing or using any undocumented Software or any Software not in strict compliance with any documentation provided to you by Sift;
5. reverse engineer, modify, adapt, or hack the Sift Services, or otherwise attempt to gain unauthorized access to the Sift Services;
6. participate in spidering, screen-scraping, database-scraping, harvesting e-mail addresses, wireless addresses, other contact or personal information, or other content made available through the Sift Services, or use any other automatic means of obtaining lists of users or other information from or through the Sift Services, including without limitation any information residing on any server or database connected to the Sift Services;
7. copy, modify, or distribute the computer code used to generate web pages on the Sift Services, except to the extent such restriction is not allowed by applicable laws, rules or regulations;
8. access, tamper with, or use non-public areas of the Sift Services, Sift's computer systems, or the technical delivery systems of Sift's providers;
9. access or search the Sift Services with any engine, software, tool, agent, device, or mechanism other than the software or search agents provided by Sift or other generally available third-party web browsers;
10. probe, scan, or test the vulnerability of any system or network, or breach any security or authentication measures;
11. benchmark, test the capacity or limitations of, or interfere with the access of any user, host or network, including, without limitation, sending a virus, overloading, flooding, spamming, or mail-bombing the Sift Services;
12. upload, post, transmit, or otherwise make available any content or information designed to interrupt, interfere with, destroy or limit the functionality of any computer software or hardware or telecommunications equipment, including the introduction of malicious code, such as viruses, worms, time bombs, or Trojan horses;
13. using any Software provided by Sift for any purpose other than your implementation of the Sift Services under the terms of the Agreement; or

14. using any data obtained through any Sift SDK-enabled application in any way the violates any individual's rights or any carrier requirements or other industry standards.