

Acceptable Use Policy

By creating/using User Accounts and/or by placing, storing and/or submitting Your data/content (“Customer Data”) into or on the Showpad SaaS Solution, you (“You” or “Your”), including the users authorized by you (“Users”) acknowledge and agree that this Acceptable Use Policy (“AUP”) shall apply in full.

The examples described in this AUP are not exhaustive. We may modify this Policy at any time by posting a revised version on Showpad’s Site. By using the Showpad SaaS Solution, You agree to the latest version of this AUP.

1. Compliance with laws

You shall comply with all applicable laws and regulations in connection the use of the Showpad SaaS Solution (including without limitation all data protection laws and regulations that may apply to you (e.g. as being the data controller), and the laws and regulations concerning the protection of intellectual and industrial property rights).

2. User Accounts

You are solely and fully responsible (including in respect of the consequences thereof) for:

- Creating and managing User Accounts;
- Ensuring that no false or misleading personal information about a User is being used for the User Account;
- all use or abuse made by the User of the User Account;
- any acts that occur in or are performed under the User Accounts;
- the safe handling, storage, confidentiality and proper usage of the User Accounts, including in respect of the User identifications, login credentials and/or passwords.

You shall use such generally accepted, reasonable and applicable knowledge, techniques, practices, technology and/or methodologies that have a proven reliably in the applicable field of industry to prevent unauthorized access to the Showpad SaaS Solution by its Users, as well as to prevent unauthorized access to the User Accounts by any third party. You shall notify Showpad promptly of any such unauthorized access or use, and employ all such means to immediately stop any such unauthorized use or misuse.

Each User shall have a designated User Account. No User shall allow any other party, or share with any party, access to the Showpad SaaS Solution through such User’s own User Account.

3. Customer Data

By using the Showpad SaaS Solution in respect of the Customer Data, you understand that such Customer Data is to be:

- (1) used and/or processed by the Showpad SaaS Solution; and/or
- (2) made accessible to Your Users and/or third parties as allowed by You or Your Users, through the Showpad SaaS Solution.

3.1 No Illegal, Harmful, or Offensive Use or Customer Data

You may not use, encourage, promote, facilitate or instruct others to use, the Showpad SaaS Solution for:

- any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available illegal, harmful, or offensive Customer Data (including activities that may be harmful to Showpad’s reputation, offering or disseminating fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming), as well as practices violating general good conduct).
- Customer Data that infringes or misappropriates the intellectual property or proprietary rights of others.
- Customer Data that is defamatory, misleading, obscene, abusive, invasive of privacy, or otherwise objectionable, including Customer Data that constitutes pornographic content, indecent content, or content that contains extreme acts of violence, or advocate hatred against any person or group of people based on their race, religion, ethnicity, sex, gender identity, sexual preference, disability, or impairment;
- Customer Data or other computer technology that may damage, interfere with, overloads, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots.

3.2 No Security Violations

You may not use the Showpad SaaS Solution to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a “System”). Prohibited activities include:



- Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.
- Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.

3.3 No Network Abuse

You may not engage in any activities which are considered to be abuse of network or abuse of network connections. Prohibited activities include:

- Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.
- Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective (Denial of Service (DoS)).
- Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.
- Operating network services like open proxies, open mail relays, or open recursive domain name servers.
- Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions.

3.4 No E-Mail or Other Message Abuse

You will not distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like “spam”). You will not alter or obscure mail headers or assume a sender’s identity without the sender’s explicit permission. You will not collect replies to messages sent from another internet service provider if those messages violate this AUP or the acceptable use policy of that provider.

3.5 No unintended use of the Showpad SaaS Solution

The Showpad SaaS Solution are intended to act as a “content activation platform” (not for instance as a backup service). Consequently, You are responsible for ensuring that master copies of Your Customer Data are stored/backed-up on Your own systems.

4. Showpad Monitoring and Enforcement

You are solely responsible for exercising supervision and control over the Users, the User Accounts, the Customer Data, as well as the Users’ or third Parties’ compliance with Your policies and procedures.

Showpad reserves the right, but does not assume any obligation or responsibility whatsoever in respect of:

- monitoring or investigating, i) any of Your User’s access to, or use of the Showpad SaaS Solution (including the management of the User Accounts) or ii) any of third parties authorized by You or Your Users to access the Customer Data;
- notify You of any misuse of the Showpad SaaS Solution or non-compliance under this AUP; or
- policing or enforcing the terms of the license(s) or permission(s) You have chosen to offer to the third parties in respect of the Customer Data, or responsibilities related to the rights, access or license granted by You to third parties in respect of the Customer Data.

Showpad may however:

- investigate violations of this AUP or misuse of the Showpad SaaS Solution;
- remove, disable access to, or modify any Customer Data or resource that violates this AUP or any other agreement Showpad has with You for use of the Showpad SaaS Solution; or
- may report any activity that Showpad suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate user information. Showpad also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

5. Reporting of Violations

If You become aware of any violation of this AUP, You will immediately notify Showpad and provide Showpad with assistance, as requested, to stop or remedy the violation.

