# DataGlyphic Acceptable Use Policy

**Note:** Last revision: January 29, 2024

Usage of DataGlyphic Cloud Services is subject to this Acceptable Use Policy (AUP). This AUP is incorporated by reference into and governed by the DataGlyphic Enterprise Subscription Agreement between you (Customer) and DataGlyphic Inc. Customers who are found to be violating these rules may see their subscriptions **suspended without prior notice**. The subscription fees will usually **not** be refunded.

---

### Illegal or Harmful Use

You may not use DataGlyphic Cloud services for storing, displaying, distributing or otherwise processing illegal or harmful content. This includes:

- **Illegal Activities:** promoting gambling-related sites or services, or child pornography.
- **Harmful or Fraudulent Activities:** Activities harmful to others, such as promoting fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, ponzi and pyramid schemes, phishing, false advertising, ...), or engaging in other deceptive practices.
- **Infringing Content:** Content that infringes the intellectual property of others.
- **Offensive Content:** Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.
- **Harmful Content:** Malicious and malware content, such as viruses, trojan horses, worms, etc.
- **Deceptive Links:** Links that deceive users into visiting malicious or dangerous websites, gather affiliate visitors/clicks, or artificially inflate the reputation of other websites.
- **Spam Content:** Content that is published for "black hat SEO" purposes, using tricks such a link building / link spam, keyword spam, in order to exploit the reputation of DataGlyphic services for promoting third-party content, goods or services.

---

### Email Abuse

You may not use DataGlyphic Cloud services for spamming. This includes:

- **Unsolicited messages:** sending or facilitating the distribution of unsolicited bulk emails and messages, either directly via DataGlyphic Cloud or indirectly via third-party email services. This includes the use of bulk emails lists. Any mass-mailing activity is subject to the applicable legal

restrictions, and you must be able to show evidence of consent/opt-in for your bulk email distribution lists.

- **Spoofing:** sending emails or messages with forged or obfuscated headers, or assuming an identity without the sender's permission

---

**Security Violations**

You may not attempt to compromise DataGlyphic Cloud services, to access or modify content that does not belong to you, or to otherwise engage in malicious actions:

- **Unauthorized access:** accessing or using any DataGlyphic Cloud system or service without permission
- **Security research:** conducting any security research or audit on DataGlyphic Cloud systems without written permission to do so, including via scanners and automated tools. Please request our Responsible Disclosure notice for more information regarding DataGlyphic security research.
- **Eavesdropping:** listening to or recording data that does not belong to you without permission
- **Other attacks:** non-technical attacks such as social engineering, phishing, or physical attacks against anyone or any system

---

**Network and Services Abuse**

You may not abuse the resources and systems of DataGlyphic Cloud. In particular the following activities are prohibited:

- **Network abuse:** causing Denial of Service (DoS) by flooding systems with network traffic that slows down the system makes it unreachable, or significantly impacts the quality of service
- **Unthrottled RPC/API calls**: sending large numbers of RPC or remote API calls to our systems without appropriate throttling, with the risk of impacting the quality of service for other users.

  **Note**: DataGlyphic provides batch APIs for imports, so there should be no need for this. Throttled calls are typically acceptable for unsustained usage at a rate of 1 call/second, with no parallel calls. Exceptions may be authorized on a case-by-case basis for DataGlyphic Online (please contact us if you think you need one), on DataGlyphic.sh the dedicated hosting mode can be considered as an alternative to this restriction.
- **Overloading:** voluntarily impacting the performance or availability of systems with abnormal content such as very large data quantities, or very large numbers of elements to process, such as email bombs.
- **Crawling:** automatically crawling resources in a way that impacts the availability and performance of the systems

- **Attacking:** using the DataGlyphic Cloud services to attack, crawl or otherwise impact the availability or security of third-party systems
- **Abusive registrations:** using automated tools to repeatedly register or subscribe to DataGlyphic Cloud services, or registering or subscribing with fake credentials, or under the name of someone else without their permission.

---

Reporting Abuse

Reports for any abusive behavior using DataGlyphic services may be sent to the responsible team via email at abuse@DataGlyphic.com