

Acceptable Use Policy

Last updated: 17 June 2026

This Acceptable Use Policy applies to the use of **Office.EU**, including by consumers, business customers, organisations, administrators, invited users, guests, and end users. It applies to our online office tools, collaboration features, file storage, synchronization, sharing functionality, APIs, websites, and related services (hereinafter: the “Services”).

By using the Service, you agree not to misuse the Services or assist anyone else in doing so.

1. General Principles

You may use the Services only for lawful, legitimate, and authorized purposes. You are responsible for all content you upload, create, store, process, share, transmit, or otherwise make available through the Services.

You must ensure that your use of the Services does not:

- violate applicable laws or regulations;
- infringe the rights of others;
- compromise the security, integrity, availability, or performance of the Services;
- expose others to harmful, abusive, deceptive, or unlawful content;
- interfere with other users’ use of the Services.

2. Illegal or Harmful Content

You must not use the Services to create, upload, store, share, publish, distribute, or facilitate access to content that is unlawful or harmful, including content that:

- promotes, facilitates, or constitutes criminal activity;
- contains child sexual abuse material or any content exploiting or endangering minors;
- promotes terrorism, violent extremism, or unlawful violence;
- contains credible threats, incitement to violence, or instructions for causing physical harm;
- is defamatory, fraudulent, deceptive, or unlawfully misleading;
- violates export control, sanctions, anti-money laundering, or anti-corruption laws;
- unlawfully includes personal data, confidential information, trade secrets, or privileged information.

3. Intellectual Property and Third-Party Rights

You must not use the Services to infringe or misappropriate intellectual property or other rights of third parties.

This includes, without limitation, using the Services to upload, store, share, distribute, or make available content that infringes copyright, database rights, trademarks, patents, trade secrets, moral rights, privacy rights, publicity rights, or contractual rights.

You must not use the Services as a repository or distribution platform for pirated software, unauthorized copies of copyrighted works, circumvention tools, license keys, cracks, or similar materials.

4. Malware, Security Abuse, and System Interference

You must not use the Services to compromise, disrupt, or interfere with systems, networks, accounts, or data.

Prohibited activities include:

- uploading, storing, distributing, or transmitting malware, ransomware, viruses, worms, trojans, spyware, or other malicious code;
- phishing, credential theft, social engineering, impersonation, or account takeover attempts;
- probing, scanning, penetration testing, vulnerability testing, or load testing without our prior written authorization;
- attempting to bypass authentication, authorization, rate limits, access controls, storage limits, or security measures;
- interfering with the normal operation of the Services or any third-party systems;
- using the Services to conduct denial-of-service attacks, botnet activity, spam campaigns, or other abusive automation;
- exploiting bugs, vulnerabilities, or misconfigurations except as permitted under an applicable vulnerability disclosure policy.

5. Abuse of File Storage and Sharing Features

You must not use the Service's file storage, synchronization, sharing, hosting, or collaboration features in a way that abuses the Services or harms others.

Prohibited uses include:

- using the Services primarily as a public file hosting, file dumping, content delivery, backup resale, or mass distribution service unless expressly permitted by your plan;
- sharing files in a way that facilitates unlawful downloads, piracy, malware distribution, phishing, fraud, or harassment;
- using public links or shared folders to distribute prohibited content;
- attempting to obscure the nature, origin, ownership, or purpose of stored or shared files;
- creating excessive numbers of files, folders, links, versions, shares, or automated operations in a way that degrades the Service;
- storing or transmitting data that you are not authorized to possess, process, or disclose.

We may disable public links, restrict sharing, quarantine files, suspend syncing, or remove content where we reasonably believe the Services is being abused or where required by law.

6. Spam, Unsolicited Communications, and Deceptive Activity

You must not use the Services to send, generate, facilitate, or support spam, phishing, scams, or deceptive communications.

This includes:

- unsolicited bulk messaging or invitations;
- deceptive document sharing requests;
- fake login pages, credential harvesting forms, or misleading collaboration links;
- impersonating another person, company, service, or authority;
- misrepresenting the origin or purpose of a file, message, link, account, or workspace.

7. Privacy and Personal Data

You must not use the Services to unlawfully collect, store, process, disclose, or otherwise handle personal data.

In particular, you must not:

- upload or share personal data without a valid legal basis or authorization;
- use the Services for unlawful surveillance, tracking, profiling, or doxxing;
- publish or share sensitive personal data without proper authority;
- process personal data in violation of applicable data protection laws or your agreement with us.

Where you use the Services to process personal data on behalf of others, you are responsible for ensuring that your use complies with applicable privacy, confidentiality, and data protection obligations.

8. Regulated, High-Risk, or Sensitive Uses

Unless expressly agreed in writing, you must not use the Services in a way that would require us to comply with sector-specific regulatory obligations beyond those stated in our agreement with you.

This may include use of the Services as a system of record for:

- medical diagnosis, emergency medical care, or other regulated healthcare services;
- financial trading, payment processing, credit scoring, or regulated financial services;

- legal, tax, or professional advice where the Services is used as the provider of such advice;
- critical infrastructure, emergency services, aviation, nuclear facilities, or life-critical systems.

You remain responsible for determining whether the Services is suitable for your intended use.

9. Excessive or Abusive Use

You must not use the Services in a manner that is excessive, abusive, or inconsistent with the ordinary purpose of a SaaS office suite.

This includes:

- circumventing storage, bandwidth, user, API, or usage limits;
- reselling, leasing, sublicensing, or making the Services available to third parties without authorization;
- using automated tools, bots, scripts, or crawlers in a way that overloads or disrupts the Service;
- creating multiple accounts to avoid limits, enforcement actions, or payment obligations;
- mining cryptocurrency or performing resource-intensive computations unrelated to the normal use of the Service;
- using the Services in a way that imposes an unreasonable or disproportionate load on our infrastructure.

10. Account and Access Misuse

You must not:

- share account credentials except as permitted by your plan or agreement;
- access or attempt to access accounts, workspaces, files, folders, or data without authorization;
- use another person's account or identity without permission;
- interfere with administrator controls, audit logs, retention settings, or security features;
- conceal or misrepresent your identity, affiliation, location, or account information.

You are responsible for maintaining the confidentiality of your credentials and for activity conducted through your account.

11. Circumvention and Reverse Engineering

Except to the extent prohibited by applicable law, you must not:

- reverse engineer, decompile, disassemble, or attempt to derive source code from the Service;

- copy, modify, or create derivative works of the Service;
- bypass technical restrictions, metering, security controls, access limits, or licensing mechanisms;
- use the Services to build or benchmark a competing product without our prior written consent.

12. Enforcement

If we reasonably believe that you have violated this Policy, we may take appropriate action, including:

- investigating the relevant activity or content;
- issuing a warning;
- requesting that you remove or modify content;
- disabling public links or sharing features;
- quarantining, blocking, or removing content;
- suspending or restricting accounts, users, workspaces, integrations, or API access;
- terminating access to the Service;
- preserving or disclosing information where required by law or to protect users, third parties, or the Services.

Where appropriate and legally permitted, we will make reasonable efforts to notify you and provide an opportunity to remedy the violation. However, we may act without prior notice where necessary to prevent harm, comply with law, protect the Service, or address urgent security, legal, or abuse risks.

13. Reporting Abuse

You may report suspected violations of this Policy by contacting us at:

notice@office.eu

Reports should include, where available:

- the relevant file, link, account, workspace, or user information;
- a description of the suspected violation;
- supporting evidence or context;
- your contact details.

We may request additional information before taking action.

14. File Sharing and Public Distribution

The Services is not intended to operate as a general-purpose public file hosting, media streaming, torrent, warez, mirror, CDN, or anonymous file distribution service. We may restrict or disable

file sharing features where usage patterns indicate that the Services is being used primarily for these purposes.

15. Changes to this Policy

We may unilaterally update this Policy from time to time. If we make material changes, we will provide notice in accordance with our Terms of Services or applicable law. Your continued use of the Services after the effective date of an updated Policy constitutes acceptance of the updated Policy.