

Acceptable Use Policy (Version 2.2)

Created Date	9 th September 2026
Last Reviewed	22 nd October 2026 – Ethan Sebastian complaints@evoxta.com → contact@evoxta.com
Next Review Due	1 st January 2027
Staff	Imogen Payne

1. About this policy

This Acceptable Use Policy explains how customers and authorised users may use the business solutions, IT support, web hosting and related services supplied **Evoxta Business Solutions** (“Evoxta”, “we”, “us” or “our”).

It forms part of our Terms and Conditions and applies to websites, applications, accounts, systems, storage and network resources supplied or managed under your service agreement.

“You” means the customer purchasing our services. You must take reasonable steps to ensure that anyone using the services through your account follows this policy.

2. Lawful and authorised use

You must use our services lawfully and within the permissions and limits of your service agreement.

You must have the necessary rights, licences and permissions for the content, software, systems and information you ask us to host, access or manage.

You must not use our services to:

- Commit, facilitate or encourage unlawful activity;
- Defraud, impersonate or deliberately mislead others;
- Infringe copyright, trade marks or other legal rights;
- Publish unlawful threats, harassment or discriminatory abuse;
- Distribute unlawful sexual content or material involving child sexual exploitation;
- Facilitate terrorism, human trafficking or other criminal exploitation; or
- Disclose confidential or personal information without lawful authority.

3. Security and access

You must protect your accounts and credentials, use appropriate passwords and enable multi-factor authentication where required or reasonably available.

You must promptly notify us if you suspect compromised credentials, unauthorised access or misuse of our services.

You must not:

- Access accounts, systems or information without permission;
- Bypass authentication, security controls or service restrictions;
- Introduce malware, ransomware or other malicious code;
- Conduct denial-of-service attacks or deliberately disrupt services;
- Intercept communications or collect credentials without lawful authority; or
- Use compromised devices or accounts to access our services.

Security testing involving our infrastructure requires our prior written agreement on its scope and timing. Authorisation to test your own website does not automatically authorise testing of shared infrastructure or third-party systems.

4. Email and messaging

Where email or messaging forms part of your service, you must use it in accordance with applicable marketing, privacy and communications laws.

You must not use our services to:

- Send unlawful unsolicited marketing;
- Send phishing messages, fraudulent communications or malicious attachments;
- Falsify sender information or impersonate another person;
- Use unlawfully obtained contact lists; or
- Operate open relays or other configurations that enable unauthorised messaging.

You must honour applicable unsubscribe requests and objections. Bulk mailing must remain within the capabilities and limits of your agreed service.

5. Hosting and resource usage

You must keep your use within the storage, bandwidth, processing and other resource limits stated in your Order.

You must not knowingly operate workloads that materially disrupt shared infrastructure, compromise security or prevent other customers from using their services.

Activities such as cryptocurrency mining, public proxy services, bulk mailing platforms or high-volume automated processing require our prior written agreement where they are outside the agreed hosting purpose.

If usage exceeds your package, we will normally contact you to agree corrective action or an appropriate upgrade. Additional charges are governed by your service agreement.

Urgent restrictions may be applied where necessary to protect services, as explained in section 10.

6. Websites, software and content

You are responsible for the content you publish and for ensuring that your website or application complies with applicable law.

Responsibility for software updates, plugins, security configuration, backups and maintenance is allocated in your Order. You must carry out the tasks assigned to you and cooperate with reasonable action needed to address vulnerabilities.

You must not knowingly upload or retain malicious files, unlawfully obtained information or software that you are not licensed to use.

Where a website permits user-generated content, you must maintain appropriate reporting and moderation arrangements where required by law.

7. Personal information and privacy

You must have a lawful basis for collecting and using personal information through our services and provide any required privacy information.

Where applicable, you must implement appropriate cookie notices and consent controls. A policy document alone does not replace technical controls where those controls are required.

You must not use our services for unlawful surveillance, credential harvesting, doxxing or unauthorised disclosure of personal information.

Do not upload sensitive information outside the agreed service scope without first arranging appropriate safeguards.

Where Evoxta processes personal information on your behalf, the data processing terms in our agreement apply.

8. IT support and remote access

You must only request access to or changes affecting systems that you own or are authorised to manage.

You must not ask our staff to bypass licensing, conceal unlawful activity, access another person's information without authority or disable safeguards for an unlawful purpose.

Before work begins, you must tell us about relevant access restrictions, critical systems and any third-party permissions required.

9. Reporting misuse

To report suspected misuse, contact: abuse@evoxta.com

Please include the relevant website address, account details where known, a description of the concern and supporting evidence.

Do not send passwords, malicious attachments or unnecessary personal information. We can arrange a suitable method for sharing sensitive evidence.

We assess reports fairly and may request further information before taking action.

10. Investigation and enforcement

Where we reasonably believe this policy has been breached, we may investigate and take proportionate action under our service agreement.

Depending on the circumstances, this may include:

- Asking you to explain or correct the issue;
- Requiring removal of specific content;
- Restricting an affected feature;
- Temporarily suspending an affected service; or
- Terminating services for a serious or unresolved breach.

We will normally explain the concern and allow a reasonable opportunity to resolve it.

Immediate action may be necessary where there is a serious security threat, apparent unlawful activity, a legal requirement or a material risk to other users or infrastructure. Where practicable and lawful, we will notify you promptly and explain the action taken.

We will limit restrictions to what is reasonably necessary and restore affected services promptly when the reason for restriction is resolved.

Any access to information during an investigation must comply with our contractual confidentiality and data protection obligations. We may preserve or disclose information where legally required or otherwise lawfully justified.

11. Review of a decision

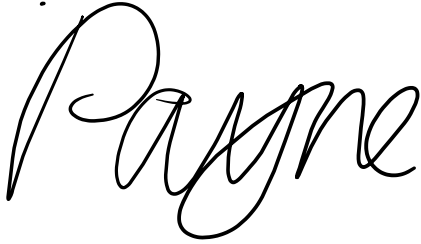
If you believe we have applied this policy incorrectly, contact us via contact@evoxta.com, explaining the decision and why you dispute it.

We will review the available information and explain our response. Review does not require us to restore access while a serious security risk or legal restriction remains.

12. Changes to this policy

Changes to this policy will be handled in accordance with the changes provisions in our Terms and Conditions.

We will publish the current version with its updated date and provide any notice or obtain any agreement required by your service contract.

A handwritten signature in black ink, reading "Payne". The signature is written in a cursive, flowing style.

Imogen Payne
Operations Manager