

OpenMail Privacy Policy

Last updated: 18 June 2026

Version: 1.0

This Privacy Policy explains how OpenMail™ Exchange, trading as OpenMail, collects, uses, stores, protects, and shares personal data when you use OpenMail, including the OpenMail web application, account area, settings, mailbox connection features, email viewing, sending, contacts, calendar, files, profile, support pages, and related services.

OpenMail is an email and productivity platform. Because email can contain private and sensitive information, this Privacy Policy is written to explain as clearly as possible what data we process, why we process it, how long we keep it, who we may share it with, and what rights you have.

Please read this Privacy Policy carefully.

1. Who we are

Service provider / trading name: OpenMail™ Exchange

Trading as: OpenMail

Business address: 41 Norman Avenue, London, N22 5ES, United Kingdom

Contact email: hello@openmail.email

Company number: Not applicable

Registered office: Not applicable — OpenMail™ Exchange is currently listed with the business address above.

VAT number: Not applicable

For data protection questions, contact:

Data protection contact: hello@openmail.email

Postal address: OpenMail™ Exchange, 41 Norman Avenue, London, N22 5ES, United Kingdom

OpenMail™ Exchange is based in the United Kingdom.

2. Scope of this Privacy Policy

This Privacy Policy applies to personal data processed through or in connection with OpenMail, including:

1. the OpenMail public website;
2. the OpenMail web application;
3. account registration and login;
4. mailbox profile settings;
5. IMAP and SMTP connection features;
6. email viewing and previews;

7. email sending;
8. Sent copy saving;
9. local contacts;
10. contact picker;
11. calendar interface;
12. files interface;
13. settings and appearance preferences;
14. profile/avatar upload;
15. support requests;
16. legal pages;
17. security logs;
18. operational logs;
19. future paid features, if introduced.

This Privacy Policy does not apply to third-party websites, mailbox providers, email providers, advertisers, hosting providers, payment providers, or external services that have their own privacy policies.

3. Key definitions

In this Privacy Policy:

“OpenMail”, “we”, “us”, and “our” means OpenMail™ Exchange, trading as OpenMail.

“You” and “your” means the person using OpenMail.

“Personal data” means information relating to an identified or identifiable person.

“Account data” means data used to create, manage, secure, and operate your OpenMail account.

“Mailbox data” means data connected to a mailbox you add to OpenMail, including mailbox address, server settings, folders, message headers, message previews, message content, sent email, and related metadata.

“Mailbox credentials” means login details or authentication secrets used to connect to your mailbox.

“Email content” means message body text, subject lines, sender information, recipient information, signatures, quoted text, and other content contained in emails.

“Contacts data” means names, email addresses, saved/unsaved contact status, contact source, last-seen information, and related contact details stored in OpenMail.

“Technical data” means device, browser, session, log, security, request, and diagnostic information.

“Processing” means anything done with personal data, including collecting, storing, using, displaying, transmitting, deleting, securing, or analysing it.

4. Our role under data protection law

For most OpenMail account, settings, security, support, legal, contact, profile, and service-operation data, OpenMail™ Exchange acts as the **data controller**. This means we decide why and how that data is processed.

For some email content and mailbox data, the position may depend on how you use OpenMail:

1. where we process data to provide your OpenMail account and mailbox-access service, we act as a controller for service operation and security;
2. where you use OpenMail to send, receive, store, or manage your own email content, you are responsible for the content you choose to process through OpenMail;
3. where you use OpenMail for business, employment, or organisation purposes, you may have your own data protection obligations in relation to people whose personal data appears in emails, contacts, files, or communications.

OpenMail does not control the content of emails you choose to send or receive.

5. Important email privacy notice

Email is private and often sensitive. Emails may contain personal data about you and others, including names, addresses, contact details, financial information, health information, family information, employment information, identity information, opinions, documents, attachments, and confidential messages.

OpenMail may process email-related data so that the service can function, including:

1. showing folders;
2. showing message lists;
3. showing sender names;
4. showing subject lines;
5. showing dates;
6. showing message previews;
7. safely displaying email content;
8. blocking remote images or unsafe content;
9. sending plain-text email;
10. saving Sent copies;
11. extracting contacts from safe header data;
12. protecting against abuse and duplicate sending.

We do not use your mailbox content to sell advertising profiles.

We do not intentionally read your emails for human review unless needed for support, security, legal compliance, abuse investigation, or troubleshooting, and only where reasonably necessary.

6. Personal data we collect directly from you

We may collect personal data you provide directly, including:

1. name;
2. display name;
3. email address;
4. OpenMail account login details;
5. password or authentication information for OpenMail;
6. mailbox email address;
7. mailbox server settings;
8. IMAP host, port, and encryption settings;
9. SMTP host, port, and encryption settings;
10. mailbox username;
11. mailbox password or mailbox authentication secret;
12. profile/avatar image;
13. theme preference;
14. density preference;
15. font preference;
16. client dark-mode preference;
17. contacts you save;
18. compose message recipients;
19. message subject;
20. message body;
21. support messages;
22. feedback;
23. legal or complaint messages;
24. account settings;
25. files you may later upload if file storage is enabled.

You should not provide personal data you do not have the right to use.

7. Personal data we collect from your connected mailbox

If you connect a mailbox, OpenMail may collect or access mailbox data such as:

1. folder names;
2. mailbox status;
3. message UIDs;
4. message flags, where needed for display;
5. sender names;
6. sender email addresses;
7. recipient email addresses where supported;
8. subject lines;
9. dates;
10. message headers;
11. safe message previews;
12. plain-text message parts;
13. safe HTML message parts;

14. attachment metadata;
15. MIME structure;
16. Sent folder detection;
17. sent message copies;
18. contact details derived from email headers.

OpenMail may block or avoid fetching certain data for privacy and safety, including:

1. remote images;
2. tracking pixels;
3. unsafe scripts;
4. unsafe HTML;
5. embedded objects;
6. attachment bodies unless a future feature clearly requires it;
7. full raw messages unless required for a specific feature.

8. Personal data we collect automatically

When you use OpenMail, we may automatically collect technical data such as:

1. IP address;
2. browser type;
3. device type;
4. operating system;
5. user agent;
6. approximate location derived from IP address;
7. request URL;
8. referrer URL;
9. timestamps;
10. session identifiers;
11. CSRF/security tokens;
12. login activity;
13. failed login activity;
14. feature usage;
15. error logs;
16. page load information;
17. performance data;
18. SMTP send timing metadata;
19. IMAP APPEND timing metadata;
20. total request timing;
21. recipient domain for safe diagnostics;
22. security events;
23. rate-limit events;
24. duplicate-send protection tokens;
25. cookie and local-storage data.

We aim to keep technical logs limited to what is needed for security, diagnostics, performance, abuse prevention, and service operation.

9. Personal data we collect from other sources

We may receive personal data from:

1. your connected mailbox;
2. your mailbox provider;
3. email senders;
4. email recipients;
5. email headers;
6. support communications;
7. hosting providers;
8. security tools;
9. error logs;
10. payment providers if paid plans are later introduced;
11. analytics or monitoring tools if enabled;
12. legal, regulatory, or abuse reports;
13. public sources where needed for fraud, security, or abuse prevention.

Where we obtain personal data from other sources, we will provide privacy information where required by law unless an exemption applies.

10. Categories of personal data we process

We may process the following categories of personal data:

1. identity data;
2. contact data;
3. account data;
4. login and authentication data;
5. mailbox profile data;
6. mailbox credentials;
7. email header data;
8. email content data;
9. email metadata;
10. contact data;
11. message sending data;
12. Sent copy data;
13. profile/avatar data;
14. preference data;
15. support data;
16. legal and complaint data;
17. device and browser data;
18. security data;
19. technical logs;
20. performance logs;
21. diagnostic data;
22. payment data if paid plans are introduced;
23. marketing preference data if marketing is introduced;
24. cookie/local-storage data.

11. Special category data

Special category data includes information about health, race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, sex life, or sexual orientation.

OpenMail does not ask you to provide special category data as part of normal account registration.

However, because OpenMail processes email and mailbox content, special category data may appear in emails, attachments, contacts, support messages, or files that you choose to send, receive, store, or process using OpenMail.

We process this data only where necessary to provide the service, where you choose to use the service for that content, where required for legal claims, where required by law, where necessary for security, or where another lawful condition applies.

You should avoid using OpenMail to process special category data unless you have a lawful basis and authority to do so.

12. Criminal offence data

Emails or files may contain criminal offence data, allegations, convictions, investigations, or related information.

OpenMail does not request criminal offence data as part of normal account use.

If criminal offence data appears in email or content you process through OpenMail, we process it only as necessary to provide the service, protect the service, comply with law, support legal claims, or where another lawful basis and condition applies.

13. Children's data

OpenMail is not intended for unsupervised use by children.

If you are under 18, you should use OpenMail only with permission from a parent or legal guardian.

We do not knowingly target children with advertising.

If we learn that a child has provided personal data without appropriate permission, we may delete or restrict the account where appropriate.

Parents or guardians may contact us at hello@openmail.email.

14. How we use personal data

We may use personal data to:

1. provide OpenMail;
2. create and manage accounts;
3. authenticate users;
4. secure accounts;
5. connect to mailboxes;
6. test mailbox connections;
7. display mailbox folders;
8. display email headers;
9. display email previews;
10. safely render message content;
11. block unsafe email content;
12. block remote images or trackers;
13. send plain-text emails;
14. save Sent copies;
15. detect Sent folders;
16. prevent duplicate sending;
17. enforce rate limits;
18. restrict sending to saved contacts;
19. block unsafe or unsaved recipients;
20. manage local contacts;
21. extract contacts from safe email header data;
22. operate contact picker features;
23. save profile/avatar images;
24. save appearance preferences;
25. save settings;
26. provide support;
27. respond to complaints;
28. investigate abuse;
29. protect mail systems;
30. prevent spam, phishing, fraud, and misuse;
31. maintain logs;
32. diagnose bugs;
33. improve service reliability;
34. maintain backups;
35. comply with legal obligations;
36. enforce our Terms;
37. protect our rights, users, and third parties;
38. provide future paid features if introduced;
39. send service notices;
40. send marketing only where allowed by law and your preferences.

15. Lawful bases for processing

We rely on different lawful bases depending on the data and purpose.

Account and service operation

Purpose: create account, log in, provide the app, keep you authenticated, provide settings.

Lawful basis: contract; legitimate interests.

Mailbox connection

Purpose: connect to your mailbox, test IMAP/SMTP, show folders and messages.

Lawful basis: contract; legitimate interests.

Mailbox credentials

Purpose: securely connect to your mailbox and send email where enabled.

Lawful basis: contract; legitimate interests.

Email viewing and previews

Purpose: show headers, previews, safe message content, folder data.

Lawful basis: contract; legitimate interests.

Email sending

Purpose: send plain-text email through your connected mailbox.

Lawful basis: contract; legitimate interests.

Sent copy saving

Purpose: save a copy of sent email to the Sent folder where supported.

Lawful basis: contract; legitimate interests.

Contacts

Purpose: store saved/unsaved contacts, extract contacts from email headers, provide contact picker.

Lawful basis: contract; legitimate interests.

Profile/avatar

Purpose: display profile image and account identity in the app.

Lawful basis: contract; consent where appropriate.

Preferences

Purpose: remember theme, density, font, dark mode, and interface choices.

Lawful basis: contract; legitimate interests; consent where required for non-essential storage.

Security and abuse prevention

Purpose: protect OpenMail, users, mail servers, and third parties.

Lawful basis: legitimate interests; legal obligation.

Logs and diagnostics

Purpose: troubleshoot errors, measure performance, detect abuse, improve reliability.

Lawful basis: legitimate interests.

Support

Purpose: respond to support requests, complaints, and legal requests.

Lawful basis: contract; legitimate interests; legal obligation.

Legal compliance

Purpose: comply with laws, court orders, regulator requests, tax, accounting, dispute, or legal obligations.

Lawful basis: legal obligation; legitimate interests.

Marketing

Purpose: send updates, newsletters, or marketing if introduced.

Lawful basis: consent or legitimate interests where allowed; PECR compliance where electronic marketing is involved.

16. Legitimate interests

Where we rely on legitimate interests, our interests may include:

1. operating OpenMail;
2. securing the service;
3. preventing spam and abuse;
4. protecting email deliverability;
5. preventing duplicate sends;
6. preventing fraud;
7. diagnosing technical issues;
8. improving product reliability;
9. protecting users;
10. protecting third parties;
11. enforcing Terms;
12. defending legal claims;
13. maintaining business records;
14. ensuring safe use of connected mailboxes.

We balance these interests against your rights and freedoms.

You may object to processing based on legitimate interests in certain circumstances.

17. Consent

We may rely on consent for certain optional features, including:

1. optional cookies;
2. analytics, if enabled;
3. marketing communications, where required;
4. profile/avatar upload, where appropriate;
5. optional future integrations;
6. optional data-sharing features;
7. optional advertising personalisation, if introduced.

Where processing is based on consent, you can withdraw consent at any time.

Withdrawing consent does not affect processing that happened before withdrawal.

18. Contract necessity

Some processing is necessary to provide OpenMail. If you do not provide required data, we may not be able to provide the service.

For example:

1. we need account data to let you log in;
 2. we need mailbox settings to connect your mailbox;
 3. we need mailbox credentials to access IMAP/SMTP features;
 4. we need recipient and message data to send email;
 5. we need session cookies to keep you logged in.
-

19. Email content and privacy

OpenMail may process email content so that you can view and send messages.

This may include:

1. subjects;
2. sender details;
3. recipient details;
4. message body;
5. quoted replies;
6. signatures;
7. safe HTML;
8. plain text;
9. MIME structure;
10. attachment metadata.

OpenMail may sanitise or change how email content appears to protect privacy and security.

OpenMail may block:

1. scripts;
2. iframes;
3. forms;
4. embedded objects;
5. unsafe links;
6. remote images;
7. tracking pixels;
8. unsafe HTML;
9. unknown active content.

OpenMail is not responsible for the privacy practices of senders whose emails you receive.

20. Remote images and tracking pixels

Many emails contain remote images or tracking pixels that can tell a sender when, where, or how an email was opened.

OpenMail may block or replace remote images by default for privacy and security.

If future features allow you to load remote images, you understand that this may disclose information to the sender or third-party image host, such as:

1. IP address;
 2. device information;
 3. approximate location;
 4. time of opening;
 5. email open event.
-

21. Attachments

OpenMail may display attachment metadata, such as filename, file type, size, and attachment status.

OpenMail may not fetch or display attachment content unless a feature clearly allows it.

If attachment features are introduced, attachments may contain personal data, malware, confidential data, or special category data.

You should only open attachments from trusted sources.

22. Sent messages

When you send an email using OpenMail, we process:

1. sender email address;

2. recipient email address;
3. subject;
4. message body;
5. sending timestamp;
6. Message-ID;
7. SMTP result;
8. recipient domain for safe diagnostics;
9. Sent folder information;
10. Sent copy status;
11. duplicate-send token;
12. rate-limit status.

OpenMail currently restricts sending to your own mailbox and saved contacts, unless later changed.

OpenMail may save a plain-text copy to the Sent folder using controlled IMAP APPEND after SMTP succeeds.

23. Contacts

OpenMail may store local contacts.

Contact data may include:

1. name;
2. email address;
3. normalised email address;
4. saved/unsaved status;
5. source, such as header or manual;
6. last seen date;
7. notes if introduced;
8. timestamps.

Contacts may be created from email headers.

Unless clearly stated otherwise, OpenMail contacts are local to OpenMail and are not synchronised with Mail-in-a-Box, CardDAV, Google Contacts, Apple Contacts, Microsoft contacts, phone contacts, or other third-party contact services.

24. Calendar data

OpenMail may provide calendar interface features.

If calendar features are placeholder-only, no real calendar sync may occur.

If future calendar features are introduced, we may process:

1. event titles;
2. event descriptions;

3. event dates and times;
4. attendees;
5. reminders;
6. locations;
7. calendar preferences;
8. sync data.

Any future calendar sync may require updated privacy information.

25. Files data

OpenMail may provide file interface or future storage features.

If file storage is enabled, we may process:

1. file names;
2. file types;
3. file sizes;
4. upload dates;
5. storage paths;
6. file metadata;
7. file content;
8. access logs;
9. deletion records;
10. storage provider metadata.

If Wasabi S3 or another storage provider is added later, data may be processed by that storage provider under its own terms and privacy policy.

You should not upload unlawful, malicious, infringing, or highly sensitive files unless you have the right and a lawful basis to do so.

26. Profile/avatar images

If you upload a profile picture, we may process:

1. the image file;
2. file name generated by OpenMail;
3. file type;
4. file size;
5. storage path;
6. upload timestamp;
7. removal timestamp if removed.

Profile images may be visible in your account interface.

You should not upload images of other people unless you have permission.

You should not upload unlawful, offensive, infringing, or misleading images.

27. Support and complaints

If you contact support, we may process:

1. your name;
2. email address;
3. account details;
4. support message;
5. screenshots;
6. error messages;
7. technical logs;
8. mailbox status;
9. correspondence history;
10. outcome notes.

Do not send passwords, private keys, full mailbox secrets, or unnecessary sensitive information in support messages.

28. Cookies, sessions, and local storage

OpenMail may use cookies, session storage, local storage, and similar technologies.

These may be used for:

1. login sessions;
2. CSRF protection;
3. authentication security;
4. theme preference;
5. density preference;
6. font preference;
7. dark-mode setting;
8. local draft placeholders;
9. interface state;
10. feature preferences;
11. security controls;
12. performance diagnostics.

Strictly necessary cookies are needed to provide the service and keep it secure.

If OpenMail introduces analytics, advertising, or non-essential cookies, we will provide information and obtain consent where required.

You can control cookies through your browser, but disabling essential cookies may stop OpenMail working.

29. Analytics

OpenMail may currently operate without third-party analytics.

If analytics are introduced, we will update this Privacy Policy and any cookie notice where required.

Analytics may process data such as page views, device type, browser, approximate location, referrer, and interaction events.

We will not use analytics to read your email content.

30. Advertising

OpenMail may show advertising placeholders or sponsored areas.

If real advertising is introduced, we may process data to display, measure, limit, or report advertising.

We do not currently use your email content to build advertising profiles.

If personalised advertising, ad networks, tracking pixels, or third-party ad technology are introduced, we will update this Privacy Policy and provide consent controls where required.

31. Marketing communications

We may send service messages, security notices, product updates, legal notices, or account-related messages.

We may send marketing messages only where allowed by law.

You can opt out of marketing messages where required.

Opting out of marketing does not stop service, security, legal, account, or transactional messages.

OpenMail is not a bulk email marketing platform.

32. Automated decision-making and profiling

OpenMail does not currently make decisions with legal or similarly significant effects about you based solely on automated processing.

OpenMail may use automated technical rules for:

1. login protection;
2. CSRF protection;
3. rate limiting;

4. duplicate-send prevention;
5. recipient restrictions;
6. blocked send attempts;
7. abuse prevention;
8. suspicious activity detection;
9. remote image blocking;
10. safe HTML sanitisation.

These are used to protect the service and do not involve profiling for advertising based on email content.

33. Who we share personal data with

We may share personal data with:

1. hosting providers;
2. server infrastructure providers;
3. mailbox servers you connect;
4. SMTP servers used to send email;
5. IMAP servers used to fetch and append messages;
6. storage providers if file/avatar storage is used;
7. security providers;
8. backup providers;
9. email recipients you choose;
10. support providers if used;
11. payment providers if paid plans are introduced;
12. professional advisers;
13. insurers;
14. legal advisers;
15. regulators;
16. law enforcement where legally required;
17. courts or dispute-resolution bodies;
18. business transfer parties if the service is sold or reorganised.

We do not sell your email content.

We do not sell mailbox credentials.

34. Mailbox providers and email recipients

When you connect a mailbox, your mailbox provider continues to process your mailbox data under its own terms and privacy policy.

When you send an email, the email may be processed by:

1. your SMTP server;
2. receiving mail servers;
3. spam filters;

4. DNS systems;
5. security gateways;
6. recipient mail providers;
7. the recipient;
8. any forwarding or filtering systems.

Email is a distributed system. Once an email leaves OpenMail or your mailbox server, we cannot control every copy, recipient, forwarding event, spam filter, or server.

35. Third-party links

Emails and OpenMail pages may contain links to third-party websites.

We are not responsible for third-party privacy practices.

You should read third-party privacy policies before providing data to them.

36. International transfers

OpenMail is operated from the United Kingdom.

Some providers, infrastructure, email recipients, mail servers, storage services, or support tools may process data outside the United Kingdom.

Where personal data is transferred internationally, we will take steps required by applicable data protection law, which may include:

1. adequacy regulations;
2. UK International Data Transfer Agreement;
3. UK Addendum to EU Standard Contractual Clauses;
4. contractual safeguards;
5. technical safeguards;
6. risk assessments.

Email may naturally travel through servers in different countries depending on mail routing and recipient providers.

37. How long we keep personal data

We keep personal data only as long as reasonably needed for the purposes described in this Privacy Policy, unless a longer period is required for legal, security, backup, accounting, dispute, or compliance reasons.

Indicative retention periods:

Account data

Kept while your account is active and for a reasonable period after closure.

Mailbox profile data

Kept while your mailbox is connected or until you remove it, subject to backup and legal retention.

Mailbox credentials

Kept only while needed to provide mailbox features, unless removed earlier by you.

Email headers and previews

Normally fetched for display and may be stored only where needed for local app features, caching, diagnostics, contacts, or support.

Sent copies

Stored in your mailbox Sent folder where APPEND succeeds. Retention is mainly controlled by your mailbox provider and your mailbox settings.

Contacts

Kept while your account exists or until deleted/unsaved, subject to backup and legal retention.

Avatar images

Kept until replaced, removed, or account closure, subject to backup and legal retention.

Preferences

Kept while your account exists or until reset.

Support messages

Typically kept for up to 6 years where needed for records, disputes, and legal protection, unless a shorter period is appropriate.

Security logs

Typically kept for a limited period needed for security, abuse prevention, and diagnostics, unless needed longer for investigation or legal reasons.

Backups

Backup copies may persist for a limited period before being overwritten or deleted.

Legal and dispute records

Kept as long as necessary for legal, regulatory, tax, accounting, or dispute purposes.

38. Deleting data

You may request deletion of your account or certain personal data by contacting hello@openmail.email.

Deletion may not be immediate where data is:

1. needed to provide the service;
2. stored in your mailbox provider's systems;
3. stored in sent/received email copies outside our control;
4. required for legal compliance;
5. required for security;
6. required for disputes;
7. stored in backups pending normal deletion cycles;
8. needed to protect rights or prevent abuse.

Deleting your OpenMail account does not delete your mailbox with your mailbox provider.

Deleting a contact in OpenMail does not necessarily delete the same contact from another service.

Deleting an email in your mailbox may depend on your mailbox provider and mail client behaviour.

39. Your data protection rights

Depending on the circumstances, you may have the right to:

1. be informed about how your data is used;
2. access your personal data;
3. correct inaccurate personal data;
4. request deletion of personal data;
5. restrict processing;
6. object to processing;
7. request data portability;
8. withdraw consent;
9. complain to the ICO;
10. challenge certain automated decisions if applicable.

These rights are not absolute and may depend on the legal basis, data type, and circumstances.

40. How to exercise your rights

To exercise your rights, contact:

Email: hello@openmail.email

Address: OpenMail™ Exchange, 41 Norman Avenue, London, N22 5ES, United Kingdom

We may need to verify your identity before responding.

We aim to respond within one month where required by law.

If your request is complex or you make multiple requests, we may need extra time where allowed by law.

41. Right of access

You may request a copy of personal data we hold about you.

We may ask for information to confirm your identity and locate your data.

We may refuse or limit access where exemptions apply, including where disclosure would affect the rights and freedoms of others.

42. Right to rectification

You may ask us to correct inaccurate personal data.

You can update some account settings directly in OpenMail.

43. Right to erasure

You may ask us to delete personal data in certain circumstances.

We may not be required to delete data where we still need it for legal, security, contractual, dispute, or legitimate reasons.

44. Right to restrict processing

You may ask us to restrict processing in certain circumstances.

Where processing is restricted, we may continue storing the data but limit other uses.

45. Right to data portability

Where applicable, you may ask to receive certain personal data in a structured, commonly used, machine-readable format.

This right applies only in certain circumstances.

Email export from your mailbox may be controlled by your mailbox provider.

46. Right to object

You may object to processing based on legitimate interests.

We may continue processing where we have compelling legitimate grounds or where processing is needed for legal claims.

You may object to direct marketing at any time.

47. Withdrawing consent

Where we rely on consent, you may withdraw consent at any time.

Withdrawal does not affect processing already carried out before withdrawal.

Some features may stop working if consent is withdrawn.

48. Complaints to the ICO

You have the right to complain to the UK Information Commissioner's Office.

ICO website: ico.org.uk

ICO helpline: 0303 123 1113

We would appreciate the opportunity to handle your concern first, so you may contact us at hello@openmail.email.

49. Security

We use appropriate technical and organisational measures designed to protect personal data.

These may include:

1. HTTPS;
2. authentication;
3. CSRF protection;
4. password hashing for OpenMail accounts;
5. encryption for stored mailbox passwords where supported;
6. access controls;
7. session controls;
8. rate limiting;
9. duplicate-send protection;
10. recipient restrictions;
11. safe HTML rendering;
12. remote image blocking;

13. attachment restrictions;
14. limited diagnostic logging;
15. server hardening;
16. backups;
17. update and patch processes;
18. restriction of sensitive operational access;
19. monitoring for errors and abuse;
20. separation of app server and mail server where applicable.

No online service can guarantee perfect security.

You must keep your own login details secure and tell us promptly if you suspect unauthorised access.

50. Data breach handling

If we become aware of a personal data breach, we will assess it and take appropriate action.

Where required by law, we will notify the ICO.

Where required by law, we will notify affected individuals.

We may not notify you of every minor incident if the law does not require notification and there is no material risk to your rights and freedoms.

51. Your security responsibilities

You are responsible for:

1. using a strong password;
 2. keeping your password private;
 3. securing your email account;
 4. securing your device;
 5. logging out on shared devices;
 6. avoiding phishing links;
 7. checking recipient addresses before sending;
 8. keeping backup copies of important data;
 9. changing passwords if you suspect compromise;
 10. ensuring you have rights to process data you upload, send, or store.
-

52. Data of other people in your emails

Your emails, contacts, files, and messages may contain personal data about other people.

You are responsible for ensuring that you have the right to use OpenMail to process that data.

If you use OpenMail for business, professional, family, school, organisational, or client purposes, you may have your own data protection obligations.

53. Business users

If you use OpenMail for business purposes, you are responsible for:

1. ensuring OpenMail is suitable for your use;
 2. complying with data protection laws;
 3. handling your own privacy notices where required;
 4. managing employee, customer, client, or supplier data lawfully;
 5. maintaining records where required;
 6. using appropriate safeguards;
 7. keeping independent backups;
 8. ensuring marketing email compliance;
 9. responding to data subject requests where you are the controller;
 10. ensuring your use does not breach confidentiality, professional, or regulatory obligations.
-

54. Sole trader and household use

If you use OpenMail for personal, family, household, or sole-trader purposes, you should still take care with other people's personal data.

You should not send or store information that you do not have the right to process.

55. Legal requests and disclosure

We may disclose personal data if we believe disclosure is necessary to:

1. comply with law;
2. respond to court orders;
3. respond to regulators;
4. protect legal rights;
5. prevent fraud;
6. investigate security incidents;
7. protect users;
8. protect third parties;
9. enforce our Terms;
10. prevent abuse of mail systems.

Where lawful and appropriate, we may challenge or narrow requests.

56. Service messages

We may send you service messages about:

1. account security;
2. login activity;
3. mailbox connection;
4. password or credential changes;
5. legal updates;
6. privacy updates;
7. terms updates;
8. service availability;
9. support responses;
10. billing if paid plans are introduced.

These messages are not marketing.

57. Payment data

OpenMail may not currently offer paid subscriptions.

If paid plans are introduced, payments may be processed by a third-party payment provider.

We may process:

1. plan type;
2. billing status;
3. subscription status;
4. payment reference;
5. invoice details;
6. billing contact details;
7. tax information;
8. payment-provider identifiers.

We should not store full card numbers unless clearly stated and handled through a compliant payment provider.

58. Future integrations

OpenMail may later add optional integrations, such as:

1. Wasabi S3 file storage;
2. CardDAV contacts;
3. CalDAV calendars;
4. payment providers;
5. analytics;
6. advertising;
7. AI assistance;

8. mobile apps;
9. push notifications;
10. third-party storage;
11. team accounts.

If future integrations materially change how personal data is processed, we will update this Privacy Policy where required.

59. AI features

OpenMail does not currently need to use email content for AI model training.

If AI features are introduced, this Privacy Policy should be updated before or when those features are made available.

Any AI feature should explain:

1. what data is processed;
 2. whether email content is used;
 3. whether third-party AI providers are involved;
 4. whether data is used for training;
 5. how long data is kept;
 6. whether the feature is optional;
 7. what controls users have.
-

60. Backups

OpenMail may create backups for operational, security, and disaster-recovery purposes.

Backups may contain personal data.

Backups are normally overwritten or deleted on a schedule.

We may not be able to remove individual records immediately from backups, but we will stop using deleted data in live systems where required and allow backup deletion cycles to complete.

61. Data minimisation

We aim to collect and retain only data that is needed for legitimate purposes.

For example:

1. contact extraction uses header data rather than full message bodies;
2. diagnostic timing logs avoid full message bodies;
3. recipient diagnostics may use domain only;
4. unsafe remote content may be blocked;

5. attachments may be metadata-only unless a feature requires content.

62. Passwords and mailbox secrets

OpenMail account passwords should be stored using password hashing.

Mailbox passwords or mailbox secrets may need to be stored so OpenMail can connect to your mailbox.

Where mailbox passwords are stored, we aim to store them encrypted where supported by the application.

Mailbox passwords are decrypted only where needed to connect to IMAP/SMTP.

We do not intentionally display or log mailbox passwords.

You may clear or change mailbox passwords in settings where the feature is available.

63. Operational logs

OpenMail may keep operational logs for security and reliability.

Logs may include:

1. timestamp;
2. account ID;
3. request path;
4. IP address;
5. browser information;
6. error code;
7. SMTP send status;
8. IMAP APPEND status;
9. timing values;
10. recipient domain;
11. folder name;
12. rate-limit status;
13. duplicate-token status.

Logs should not intentionally include:

1. mailbox passwords;
 2. full SMTP transcripts;
 3. full IMAP transcripts;
 4. full message bodies;
 5. private keys.
-

64. Local storage and browser-only drafts

Some OpenMail features may use browser storage.

For example, a draft toast may be a local UI feature and may not mean the draft was saved to your mailbox server.

Browser storage may be cleared if you clear browser data, use private browsing, change device, or reset settings.

Do not rely on browser-only storage as your only copy of important information.

65. Data accuracy

You should keep your account and mailbox details accurate.

You are responsible for checking recipient addresses before sending emails.

OpenMail may not detect all incorrect, outdated, or misleading contact details.

66. Data portability and export

OpenMail may introduce export features in the future.

Your connected mailbox provider may already provide export tools.

Contact us at hello@openmail.email if you need help with data access or export options.

67. Account closure

If you request account closure, we may delete or disable:

1. account data;
2. local contacts;
3. preferences;
4. avatar images;
5. mailbox profile data;
6. support access;
7. app-specific data.

Some records may be retained where required for:

1. legal compliance;
2. security;
3. fraud prevention;

4. dispute resolution;
5. backups;
6. accounting;
7. enforcement of Terms.

Closing OpenMail does not delete emails stored by your mailbox provider.

68. Changes to this Privacy Policy

We may update this Privacy Policy from time to time.

If we make material changes, we will take reasonable steps to notify users, such as by updating the app, posting a notice, changing the "Last updated" date, or sending a service message.

If you continue using OpenMail after changes take effect, the updated Privacy Policy will apply.

Where consent is required for new processing, we will seek consent where required.

69. Contact details

For privacy questions, rights requests, complaints, or concerns, contact:

OpenMail™ Exchange

41 Norman Avenue
London
N22 5ES
United Kingdom

Email: hello@openmail.email

70. Summary

OpenMail processes personal data to provide a private webmail and productivity service.

We process account data, mailbox settings, email headers, safe previews, sending data, Sent copy data, contacts, preferences, profile images, support data, and technical logs.

We use this data to operate OpenMail, connect your mailbox, display emails, send messages, save Sent copies, manage contacts, secure the service, prevent abuse, provide support, and comply with law.

We do not sell your email content.

We do not intentionally log mailbox passwords.

You have privacy rights under UK data protection law.

Contact hello@openmail.email for privacy questions or rights requests.

© 2026 OpenMail™ Exchange. All rights reserved.