

OpenMail Cookie Policy

Last updated: 18 June 2026

Version: 1.0

This Cookie Policy explains how OpenMail™ Exchange, trading as OpenMail, uses cookies, browser storage, local storage, session storage, security tokens, preference storage, and similar technologies on OpenMail websites and applications, including <https://openmail.email>, <https://app.openmail.email>, the OpenMail web application, login pages, settings pages, legal pages, and related services.

This Cookie Policy should be read together with our Terms & Conditions, Privacy Policy, Disclaimer, and Help & Support pages.

By using OpenMail, you acknowledge that we use essential cookies and similar technologies that are necessary for the service to work. Where we use non-essential cookies or similar technologies, we will explain them and request consent where required.

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

Website: <https://openmail.email>

App: <https://app.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 cookie or privacy questions, contact:

Email: hello@openmail.email

2. Purpose of this Cookie Policy

This Cookie Policy explains:

1. what cookies are;
2. what similar technologies are;
3. what cookies and storage OpenMail uses;
4. why OpenMail uses them;
5. which cookies are essential;

6. which cookies are optional or future-use only;
 7. how long cookies may last;
 8. how you can control cookies;
 9. how cookies relate to privacy and security;
 10. when consent may be needed;
 11. what happens if cookies are disabled.
-

3. What are cookies?

Cookies are small text files placed on your device by a website or web application.

Cookies can help websites:

1. keep you logged in;
2. remember your preferences;
3. protect against security attacks;
4. remember actions you have taken;
5. understand how a service is used;
6. keep sessions working;
7. support form submissions;
8. prevent duplicate or unsafe actions.

Cookies may be:

1. **session cookies** — deleted when your browser session ends;
 2. **persistent cookies** — stored for a set period;
 3. **first-party cookies** — set by OpenMail;
 4. **third-party cookies** — set by another service;
 5. **strictly necessary cookies** — needed for the service to work;
 6. **non-essential cookies** — used for analytics, advertising, personalisation, or optional features.
-

4. What are similar technologies?

Cookie rules also apply to similar technologies that store information on your device or access information from your device.

OpenMail may use technologies such as:

1. browser localStorage;
2. browser sessionStorage;
3. security tokens;
4. application session identifiers;
5. CSRF tokens;
6. preference storage;
7. theme storage;
8. density storage;
9. font storage;
10. draft placeholder storage;

11. interface state storage;
12. cache data;
13. browser storage used by the web app.

In this policy, “cookies” may also refer to these similar technologies where appropriate.

5. Current OpenMail cookie position

At the time of this policy, OpenMail is designed to use cookies and similar technologies mainly for:

1. login and session security;
2. CSRF protection;
3. keeping the web application working;
4. remembering interface preferences;
5. remembering theme/dark-mode choices;
6. remembering density choices;
7. remembering font choices where enabled;
8. supporting local draft placeholders;
9. supporting app interface state;
10. preventing unsafe or duplicate actions;
11. improving reliability and security.

OpenMail does not currently need advertising tracking cookies to provide the service.

OpenMail does not currently use email content to build advertising profiles.

OpenMail does not currently use third-party analytics cookies unless clearly introduced later.

If this changes, this Cookie Policy should be updated and consent controls should be added where required.

6. Strictly necessary cookies

Strictly necessary cookies are required for OpenMail to function.

They may be used for:

1. logging in;
2. keeping you logged in;
3. protecting forms;
4. preventing cross-site request forgery;
5. maintaining a secure session;
6. supporting authenticated app pages;
7. preventing unauthorised requests;
8. keeping basic security controls working;
9. allowing settings or mailbox actions requested by you;
10. protecting the service from misuse.

You cannot use core OpenMail account features properly without strictly necessary cookies.

These cookies do not require consent where they are essential to provide the service you requested, but we still explain them in this policy.

7. Security cookies and tokens

OpenMail may use security cookies and tokens to protect the service.

These may include:

1. session cookies;
2. CSRF tokens;
3. authentication state;
4. login protection;
5. rate-limit support;
6. duplicate-action protection;
7. form validation support;
8. secure request checks.

These help protect against:

1. unauthorised account access;
 2. forged requests;
 3. duplicate sends;
 4. abuse;
 5. session misuse;
 6. accidental repeated actions;
 7. security attacks.
-

8. Session cookies

OpenMail may use a session cookie to recognise your logged-in session.

This cookie helps OpenMail know that you have logged in and are allowed to access your account area.

Without this cookie, OpenMail may not be able to:

1. keep you logged in;
2. show your mailbox;
3. show your settings;
4. access authenticated pages;
5. process secure actions;
6. protect your account.

A session cookie usually expires when your session ends, when you log out, or after the configured session lifetime.

9. CSRF cookies or tokens

OpenMail may use CSRF cookies or tokens to protect forms and requests.

CSRF protection helps stop another website from tricking your browser into making unwanted requests to OpenMail.

This is important for actions such as:

1. logging in;
2. logging out;
3. saving settings;
4. updating profile images;
5. sending email;
6. saving contacts;
7. unsaving contacts;
8. updating preferences.

CSRF cookies or tokens are strictly necessary for security.

10. Remember-me cookies

If OpenMail later adds or enables a “remember me” feature, a persistent cookie may be used to keep you logged in for longer.

If used, this cookie may remain on your device after closing the browser.

You should not use remember-me features on shared or public devices.

If you log out, the remember-me cookie should be cleared or invalidated where possible.

11. Preference cookies and browser storage

OpenMail may use cookies or browser storage to remember interface preferences.

These may include:

1. theme;
2. dark mode;
3. light mode;
4. system theme preference;
5. density;
6. font choice;
7. selected layout;
8. sidebar state;
9. panel state;
10. selected UI preferences.

These preferences help OpenMail feel consistent when you return.

Preference storage may be account-based, cookie-based, localStorage-based, sessionStorage-based, or a mixture depending on the feature.

12. Theme storage

OpenMail may remember whether you prefer:

1. light mode;
2. dark mode;
3. system/default mode.

This may be stored in your account, localStorage, cookies, or browser storage.

If you clear cookies or browser storage, OpenMail may return to the default theme.

13. Density storage

OpenMail may remember a density setting such as:

1. comfortable;
2. compact;
3. spacious;
4. default.

Density controls how much spacing appears in the interface.

This may be stored in your account or browser storage.

14. Font storage

OpenMail may allow you to choose a font style.

Font preference may be stored to apply your chosen font across the app.

OpenMail should use safe CSS font stacks unless external fonts are clearly introduced later.

If browser storage is cleared, your font preference may reset.

15. Draft and compose storage

OpenMail may use local or session browser storage for draft-related interface features.

For example, OpenMail may show a “Saved to Drafts” toast when you close a compose window that contains message body text.

Unless clearly stated otherwise:

1. draft storage may be local/browser-only;
2. draft storage may not be saved to the mailbox server;
3. local draft data may be cleared if browser storage is cleared;
4. local draft data may not appear on another device;
5. local draft data may not appear in other mail clients.

Do not rely on browser-only draft storage as the only copy of important messages.

16. Contact picker and interface state

OpenMail may store temporary interface state for:

1. compose window state;
2. contact picker state;
3. selected tab;
4. selected folder;
5. selected message;
6. panel expansion state;
7. toast/notification visibility;
8. full email view state.

This may be stored temporarily in memory, sessionStorage, localStorage, or account preferences.

Some of this data may disappear when you refresh, log out, close the browser, or clear browser storage.

17. Rate-limit and duplicate-send support

OpenMail may use server-side state, request tokens, cookies, or session data to help enforce:

1. send rate limits;
2. duplicate-send protection;
3. safe resend behaviour;
4. CSRF protection;
5. validation flow;
6. abuse prevention.

This helps protect users, recipients, and mail systems.

18. Avatar and profile image storage

OpenMail may store your profile image on the server rather than using cookies.

However, cookies or browser cache may help display the image efficiently.

If you update or remove your avatar, your browser may briefly show a cached version until refreshed.

19. Legal pages and public pages

OpenMail legal pages may use minimal essential cookies or storage for:

1. theme;
2. accessibility;
3. security;
4. navigation state;
5. session detection;
6. authenticated/public link display.

Public legal pages should not require advertising or analytics cookies unless those features are introduced later.

20. Current expected OpenMail cookies and storage

The exact cookie names may vary depending on the application configuration, Laravel session configuration, browser, deployment settings, and future updates.

OpenMail may use cookies or storage similar to the following:

Name or type	Category	Purpose	Typical duration
OpenMail session cookie	Strictly necessary	Keeps you logged in and maintains secure app session	Session or configured session lifetime
CSRF token cookie or token	Strictly necessary	Protects forms and requests from cross-site request forgery	Session or configured token lifetime
Remember-me cookie, if enabled	Strictly necessary / account access	Keeps you logged in for longer if selected	Persistent until expiry or logout
Theme preference	Preference	Remembers light/dark/system theme	Until changed or storage cleared
Density preference	Preference	Remembers compact/comfortable layout	Until changed or storage cleared
Font preference	Preference	Remembers chosen UI font style	Until changed or storage cleared
Compose/draft placeholder state	Functionality	Supports local draft UI behaviour	Session, local, or until cleared

Name or type	Category	Purpose	Typical duration
Sidebar/panel/UI state	Functionality	Remembers app layout preferences	Session, local, or until cleared
Rate-limit/duplicate action token	Security/functionality	Helps prevent duplicate sends or abuse	Short-lived
Browser cache	Functionality/performance	Helps assets load faster	Controlled by browser/cache headers

Before final publication, OpenMail should verify exact live cookie names in the browser developer tools and update this table if needed.

21. Analytics cookies

OpenMail does not currently need analytics cookies to provide the core email service.

If analytics are introduced in the future, this policy should be updated to explain:

1. the analytics provider;
2. what data is collected;
3. why it is collected;
4. whether cookies are used;
5. how long data is kept;
6. whether data is shared internationally;
7. how users can accept or reject analytics;
8. how consent can be withdrawn.

Analytics cookies should not be set unless the required consent has been obtained, where consent is required.

22. Advertising cookies

OpenMail may display advertisement placeholders or sponsored areas.

Placeholder adverts should not use advertising cookies, tracking pixels, ad networks, or remote ad scripts.

If real advertising is introduced later, OpenMail should update this policy to explain:

1. whether advertising cookies are used;
2. whether ads are personalised;
3. which partners or ad networks are involved;
4. what data is collected;
5. whether email content is used for ads;
6. how users can control advertising cookies;

7. how consent is requested;
8. how consent can be withdrawn.

OpenMail does not currently use your email content to build advertising profiles.

23. Third-party cookies

OpenMail should avoid third-party cookies unless needed for a clearly explained feature.

Third-party cookies may be introduced in the future for:

1. payments;
2. analytics;
3. support tools;
4. security tools;
5. advertising;
6. embedded media;
7. external integrations.

If third-party cookies are introduced, this policy should identify the third party, explain the purpose, and provide controls where required.

Third-party providers may have their own privacy and cookie policies.

24. Payment cookies

OpenMail may not currently offer paid plans.

If paid plans are introduced, payment providers may use cookies or similar technologies for:

1. fraud prevention;
2. checkout security;
3. payment processing;
4. subscription management;
5. tax calculation;
6. invoicing;
7. customer authentication.

Payment-provider cookies may be controlled by the payment provider and explained in their own policies.

25. Support and chat cookies

OpenMail may not currently use live chat support.

If support chat, helpdesk, or ticketing tools are introduced, they may use cookies for:

1. chat session state;
2. support ticket state;
3. user identification;
4. fraud prevention;
5. customer service history;
6. notification state.

This policy should be updated before or when such tools are introduced.

26. Security and fraud-prevention cookies

OpenMail may use cookies, tokens, logs, and security state to protect:

1. accounts;
2. sessions;
3. mailbox connections;
4. compose sending;
5. contact actions;
6. profile updates;
7. settings updates;
8. legal compliance;
9. service stability.

Security cookies are usually strictly necessary.

27. Local storage

OpenMail may use localStorage to remember settings or local UI state.

Local storage differs from cookies because it is stored in your browser and is not automatically sent with every request.

LocalStorage may be used for:

1. theme;
2. density;
3. font;
4. compose placeholder state;
5. draft UI state;
6. sidebar state;
7. account interface state;
8. recent UI choices.

Clearing browser storage may reset these settings.

28. Session storage

OpenMail may use sessionStorage for temporary page or interface state.

Session storage may be cleared when you close the tab or browser.

It may be used for:

1. temporary UI state;
 2. compose window state;
 3. selected view state;
 4. temporary navigation state;
 5. safe app behaviour during a session.
-

29. Browser cache

Your browser may cache OpenMail assets such as:

1. CSS files;
2. JavaScript files;
3. icons;
4. logos;
5. avatar images;
6. interface assets.

Caching improves performance.

If the app looks outdated after an update, you may need to refresh the page or clear cache.

30. Server logs and cookies

Cookies and request data may appear in server logs where necessary for security and operation.

OpenMail aims not to intentionally log:

1. mailbox passwords;
2. full email bodies;
3. full SMTP transcripts;
4. full IMAP transcripts;
5. private keys;
6. recovery codes.

Operational logs may include technical data such as:

1. IP address;
2. timestamp;
3. request path;

4. browser/user agent;
 5. account ID;
 6. security event;
 7. error status;
 8. timing data;
 9. recipient domain for safe diagnostics.
-

31. Consent

OpenMail may use strictly necessary cookies without consent where they are required to provide the service you requested.

For non-essential cookies, such as analytics, advertising, tracking, or optional third-party cookies, OpenMail should request consent where required.

Consent should be:

1. freely given;
2. specific;
3. informed;
4. unambiguous;
5. given by a clear positive action;
6. easy to withdraw.

OpenMail should not use pre-ticked boxes or hidden consent for non-essential cookies.

32. Withdrawing consent

If OpenMail introduces optional cookies, you should be able to withdraw consent as easily as giving it.

This may be done through:

1. cookie settings;
2. privacy settings;
3. browser controls;
4. a cookie banner or preference centre;
5. contacting support where needed.

Withdrawing consent may disable optional features but should not stop strictly necessary cookies needed for the service.

33. Cookie banner

OpenMail may not need a cookie banner where only strictly necessary cookies and necessary local storage are used.

If OpenMail introduces non-essential analytics, advertising, tracking, or third-party cookies, a cookie banner or preference centre may be required.

A cookie banner should:

1. explain cookie purposes clearly;
2. allow rejection of non-essential cookies;
3. allow acceptance of non-essential cookies;
4. not use deceptive design;
5. not make rejection harder than acceptance;
6. allow users to change their choice later;
7. block non-essential cookies until consent is given.

34. Managing cookies in your browser

You can manage cookies through your browser settings.

Most browsers allow you to:

1. view cookies;
2. delete cookies;
3. block cookies;
4. block third-party cookies;
5. clear site data;
6. clear localStorage;
7. clear sessionStorage;
8. control tracking protection;
9. use private browsing mode.

Browser controls vary by browser.

Blocking all cookies may stop OpenMail working properly.

35. Browser-specific controls

You can usually find cookie controls in browser settings for:

1. Google Chrome;
2. Microsoft Edge;
3. Mozilla Firefox;
4. Apple Safari;
5. Brave;
6. Opera;
7. mobile browsers.

Please check your browser's official help pages for current instructions.

36. What happens if you block cookies?

If you block all cookies, OpenMail may not be able to:

1. log you in;
2. keep you logged in;
3. protect forms;
4. save settings;
5. apply theme preferences;
6. apply density preferences;
7. apply font preferences;
8. operate secure compose actions;
9. process contact save/unsave actions;
10. protect against duplicate sends;
11. maintain app state;
12. remember your choices.

Essential app features may stop working.

37. What happens if you clear local storage?

If you clear localStorage or browser site data, OpenMail may lose:

1. theme preference;
2. density preference;
3. font preference;
4. local draft placeholders;
5. compose UI state;
6. selected layout state;
7. saved browser-only choices;
8. local notification state.

Account-stored settings may remain if they are saved server-side.

38. Do cookies read my emails?

No. Cookies themselves do not read your emails.

OpenMail processes mailbox data separately to provide email features.

Cookies and similar technologies mainly help with login, security, preferences, and app functionality.

OpenMail does not use cookies to read email content for advertising profiles.

39. Do cookies send my email content to advertisers?

OpenMail does not currently use advertising cookies to send email content to advertisers.

Placeholder ads should not use tracking cookies or ad networks.

If real advertising is introduced, this policy and the Privacy Policy should be updated.

40. Do cookies affect email delivery?

Cookies do not directly affect email delivery.

However, if cookies are blocked, OpenMail may not be able to keep you logged in, validate forms, or process sending actions correctly.

41. Cookies and children

OpenMail is not intended for unsupervised use by children.

If a child uses OpenMail, essential cookies may still be needed for login and security.

Parents or guardians can contact hello@openmail.email with concerns.

42. Cookies and shared devices

If you use OpenMail on a shared device:

1. do not use "remember me" if available;
 2. log out after use;
 3. avoid saving passwords in the browser;
 4. clear cookies and site data if needed;
 5. do not leave compose windows or private messages open.
-

43. Cookies and private browsing

Private or incognito browsing may delete cookies and local storage when the session ends.

This may affect:

1. login persistence;
2. preferences;
3. local drafts;
4. interface state.

44. Cookies and VPNs, blockers, and privacy tools

VPNs, ad blockers, script blockers, privacy extensions, browser tracking protection, and corporate firewalls may affect OpenMail.

They may block:

1. cookies;
2. JavaScript;
3. localStorage;
4. sessionStorage;
5. app assets;
6. icons;
7. login sessions;
8. security tokens.

If OpenMail does not work correctly, try disabling extensions for OpenMail or using another browser.

45. Cookie review and updates

OpenMail should review cookies and storage technologies periodically.

This policy may be updated when:

1. new features are added;
2. analytics are introduced;
3. ads are introduced;
4. payments are introduced;
5. support chat is introduced;
6. third-party integrations are introduced;
7. storage behaviour changes;
8. legal requirements change;
9. cookie names or purposes change.

The “Last updated” date shows when this policy was last changed.

46. Current cookie status summary

At the time of this policy:

1. OpenMail uses essential cookies and storage for login, security, preferences, and app operation.
2. OpenMail may use localStorage/sessionStorage for theme, density, font, draft placeholders, and interface state.
3. OpenMail does not currently require third-party advertising cookies.
4. OpenMail does not currently use email content for advertising profiles.
5. OpenMail should not set non-essential analytics or advertising cookies without updating notices and obtaining consent where required.

6. Blocking essential cookies may stop the app working.

47. Relationship with the Privacy Policy

Cookies and similar technologies may involve personal data.

For more information about personal data, lawful bases, retention, sharing, and privacy rights, read the Privacy Policy at:

<https://app.openmail.email/privacy>

48. Relationship with the Terms

Your use of OpenMail is also governed by the Terms & Conditions at:

<https://app.openmail.email/terms>

The Terms explain service rules, acceptable use, account responsibilities, email sending rules, beta features, liability limits, and other important conditions.

49. Contact

Questions about this Cookie Policy should be sent to:

OpenMail™ Exchange

41 Norman Avenue
London
N22 5ES
United Kingdom

Email: hello@openmail.email

50. Short cookie summary

OpenMail uses essential cookies and similar technologies to keep you logged in, protect your session, secure forms, remember preferences, and make the app work.

OpenMail may use browser storage for theme, density, font, local draft placeholders, and interface state.

OpenMail does not currently use advertising cookies to profile users from email content.

If non-essential analytics, advertising, tracking, payment, support chat, or third-party cookies are introduced, OpenMail should update this policy and request consent where required.

