PRIVACY POLICY FOR ABLELINK SMART LIVING EMAIL WEB APPLICATION

Effective Date: June 2, 2026

This Privacy Policy explains how AbleLink Smart Living Technologies, LLC ("we", "us", or "our") collects, uses, discloses, and protects your information when you use the AbleLink Smart Living Email web application ("Web Application"), which was created by AbleLink Smart Living Technologies, LLC. The Web Application is a web-based email client that allows you to access, read, send, and manage email from your existing email accounts (including Google, Microsoft, Apple iCloud, and other email providers that support IMAP).

1. Information We Collect

a. Account and Authentication Information (via AbleLink Smart Living Manager)

The Web Application uses AbleLink Smart Living Manager ("SLM") as its single sign-on system. Your user account — including your name, username, and password — is created in and managed by SLM, not by the Web Application. When you sign in, SLM authenticates you and securely passes basic identifying information (such as your name and username) to the Web Application so that it can recognize you and load your settings, email accounts, and other Web Application data.

The handling of your name, username, and password by SLM is described in the AbleLink Smart Living Manager Privacy Policy, available at https://www.ablelinktech.com/slm-privacy-policy/.

b. Information You Provide to the Web Application

When you configure email accounts or otherwise use features of the Web Application, you may provide us with information such as:

- Email account configuration information (e.g., IMAP/SMTP server addresses, port numbers, your email account username)
- Email account credentials (e.g., IMAP/SMTP passwords, app-specific passwords for providers such as Apple iCloud)
- OAuth authorization tokens you grant when connecting Google or Microsoft email accounts
- Contacts you create within the Web Application's address book (e.g., names, email addresses, optional photos). The Web Application's contacts are maintained inside the Web Application only; they are not synchronized with the contacts list of any connected email provider.
- Preferences and settings (e.g., theme, font size, text-to-speech preferences)

- Any other information you voluntarily provide while using the Web Application

c. Email Account Content

In order to function as an email client, the Web Application accesses, transmits, and stores content from the email accounts you connect to it. This includes:

- Email messages (including subject lines, message bodies, sender and recipient addresses, dates, and other headers)
- Attachments included with email messages
- Folder and label structure of your email account
- Status information about messages (e.g., read/unread, flagged)

This content is retrieved from your email provider on your behalf and cached so that the Web Application can display, search, and organize it efficiently. Message metadata (subject lines, sender and recipient addresses, dates, flags, folder structure, and similar information) is stored in our database. Message bodies (the readable contents of your email) and attachments are stored as files on the application server's file system.

d. Automatically Collected Information

When you interact with the Web Application, we may automatically collect information about your visit, including:

- IP address
- Browser type and version
- Operating system and platform
- Pages you visit within the Web Application
- Date and time of your visit
- Referring URL (the website that directed you to our application)

We may also collect device-specific information such as device type, unique device identifiers, and network information.

2. Precise, Real-time Location Information Collection

The Web Application does not collect precise location information.

3. Cookies and Tracking Technologies

Our Web Application uses cookies and similar technologies to collect information about your interactions with our site. Cookies are small data files stored on your device that help us recognize you and are limited to functionality required by the Web Application (such as keeping you signed in). You can manage your cookie preferences in your browser settings, but disabling cookies will keep the Web Application from functioning properly.

We do not use third-party advertising cookies, analytics trackers, or error-tracking services.

4. How We Use Your Information

We use the information we collect for the following purposes:

- To provide, maintain, and improve the Web Application and its features
- To authenticate to your email provider on your behalf and retrieve, send, and manage your email
- To display, search, organize, and otherwise present your email content to you within the Web Application
- To process your requests and respond to your inquiries
- To analyze usage and trends to improve our services
- To protect the security and integrity of our Web Application and comply with legal obligations

We do not use the contents of your email for advertising. We do not sell, rent, or otherwise transfer the contents of your email to third parties for their own use. We do not use the contents of your email to train artificial intelligence or machine learning models.

5. Sharing Your Information

We do not sell your personal information to third parties.

We may share your information in the following limited circumstances:

- **Email providers.** When you use the Web Application to read or send email, your information is exchanged with the email provider whose account you have configured (for example, Google, Microsoft, Apple iCloud, or another IMAP/SMTP provider you have configured). This is inherent to the function of an email client. Your interactions with those providers are governed by their own privacy policies.
- **Hosting and infrastructure providers.** The Web Application and its database are hosted by third-party cloud infrastructure providers located in the United States. These providers supply the underlying compute, storage, and database infrastructure but do not access your data for their own purposes.
- **Legal compliance and protection.** We may disclose your information if required to do so by law, or if we believe such action is necessary to comply with legal obligations, protect the rights or safety of our users, or prevent fraud.

6. Google API Services User Data and Limited Use

If you connect a Google account (Gmail) to the Web Application, the Web Application uses Google APIs to access your email on your behalf. To do so, you will be asked through Google's standard OAuth consent flow to grant the Web Application permission to read, modify, and send mail on your behalf.

Smart Living Email's use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements.

Specifically:

- We use Google user data only to provide and improve the email-client functionality of the Web Application that is visible to you.
- We do not transfer Google user data to third parties except as necessary to provide or improve the Web Application's functionality, to comply with applicable law, or as part of a merger, acquisition, or sale of assets with appropriate notice to you.
- We do not use Google user data for serving advertisements.
- We do not allow humans to read Google user data, except (i) with your affirmative consent for specific messages, (ii) when necessary for security purposes such as investigating abuse, (iii) to comply with applicable law, or (iv) where the data has been aggregated and anonymized for use in internal operations.
- We do not use Google user data to develop, improve, or train generalized artificial intelligence or machine learning models.

You may revoke the Web Application's access to your Google account at any time by visiting your Google Account permissions page.

7. Microsoft and Apple iCloud Account Connections

If you connect a Microsoft email account (e.g., Outlook.com, Microsoft 365), the Web Application uses Microsoft's OAuth flow to obtain permission to access your mail on your behalf. We use the resulting access tokens only to provide email-client functionality to you within the Web Application. You may revoke the Web Application's access at any time through your Microsoft account's app permissions settings.

Apple iCloud does not currently support OAuth for third-party email clients. To connect an iCloud email account, you must generate an app-specific password through your Apple ID account settings and provide it to the Web Application. The Web Application stores that app-specific password in order to maintain your connection to iCloud. You may revoke access at any time by removing the app-specific password from your Apple ID account.

For other email providers connected via IMAP/SMTP, the Web Application stores the username and password (or app-specific password) you provide so that it can authenticate to your provider on your behalf.

8. Data Security

We take reasonable measures to protect your information from unauthorized access, alteration, disclosure, or destruction.

- **In transit.** All connections between your browser and the Web Application are encrypted using HTTPS/TLS with industry-standard methods and algorithms. Connections from the Web Application to your email providers are likewise encrypted.
- **At rest.** Our database is configured with encryption at rest enabled, using industry-standard methods and algorithms. In addition, the most sensitive credentials we store — IMAP and SMTP passwords, Apple iCloud app-specific passwords, and the OAuth access and refresh tokens issued by Google and Microsoft — are individually encrypted at the column level using authenticated encryption before being written to the database. Local account passwords are not stored; only a one-way hash of the password is kept. The cached message bodies and attachments that the Web Application stores on its file system are encrypted by the Web Application using authenticated encryption before being written to disk. The keys used for these encryption operations are not stored alongside the encrypted data; they are held in a separate managed key store and supplied to the Web Application at runtime. The server file system itself is also hosted on volumes that are encrypted at rest.
- **Access controls.** Access to production systems and data is restricted to authorized personnel.

However, no method of transmission over the Internet, and no method of electronic storage, is completely secure, and we cannot guarantee the absolute security of your data.

9. Data Retention

We retain your information for as long as necessary to provide the Web Application to you, or as required by law.

- **Email content and attachments** cached by the Web Application are retained until you delete the corresponding email from within the Web Application or remove the connected email account.
- **Account credentials and OAuth tokens** are retained for as long as the corresponding email account is connected to your Web Application account, and are deleted when the connection is removed or your account is closed.
- **Web Application account information** is retained for as long as your account is active. When you close your account, or when we determine that your information is no longer needed, we will securely delete it.

10. Your Rights

You have the right to:

- Access, correct, or delete your personal information stored by us

- Disconnect any email account from the Web Application at any time, which will remove the associated credentials, OAuth tokens, and cached email content from our systems
- Revoke OAuth permissions for Google or Microsoft directly through those providers, in addition to (or instead of) disconnecting the account from within the Web Application
- Withdraw consent for data collection, where applicable
- Close your AbleLink account, which is managed through AbleLink Smart Living Manager. Closing your account through SLM will result in the deletion of your Web Application data, including connected email account configurations, stored credentials and tokens, cached messages and attachments, contacts, and preferences. Information held by SLM itself (your name, username, and password) is governed by SLM's privacy policy.

To exercise any of these rights, please contact us at info@ablelinktech.com.

11. Children's Privacy

The Web Application is not directed to children under the age of 13, and we do not knowingly collect personal information from children under 13. If you believe we have collected information from a child under 13, please contact us at info@ablelinktech.com so that we can delete it.

12. Your California Privacy Rights

This section applies to residents of California and supplements the rest of this Privacy Policy. It is provided pursuant to the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA").

a. Categories of Personal Information We Collect

In the preceding twelve months, we have collected the following categories of personal information from users of the Web Application:

- **Identifiers**, such as name, email address, phone number, IP address, and account username.
- **Personal information categories listed in Cal. Civ. Code § 1798.80(e)**, such as account log-in credentials.
- **Internet or other electronic network activity information**, such as browser type, operating system, pages visited within the Web Application, and the date and time of your visits.
- **Sensitive personal information**, specifically: (i) account log-in credentials and OAuth authorization tokens used to connect your email accounts to the Web Application, and (ii) the contents of email messages stored in or transmitted through the email accounts you connect to the Web Application.

We do not knowingly collect biometric information, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, union membership, genetic data, health information, or information about sex life, sexual orientation, or criminal history.

b. Sources of Personal Information

We collect this information from:

- You directly, when you register, configure email accounts, and otherwise use the Web Application.
- Automatically, through your use of the Web Application (e.g., log files, cookies).
- The email providers you authorize the Web Application to connect to (e.g., Google, Microsoft, Apple iCloud, or other IMAP servers), when retrieving your email on your behalf.

c. Business and Commercial Purposes for Collection

We collect personal information for the purposes described in Section 4 ("How We Use Your Information"), which include providing and maintaining the Web Application, authenticating to your email providers on your behalf, securing the Web Application, and complying with legal obligations.

d. Disclosure of Personal Information

In the preceding twelve months, we have disclosed personal information for business purposes to the categories of recipients described in Section 5 ("Sharing Your Information"), including email providers, hosting and infrastructure providers acting as our service providers, and government or legal authorities where required.

e. Sale and Sharing of Personal Information

We do not sell personal information, and we do not share personal information for cross-context behavioral advertising, as those terms are defined under the CCPA. We have not done so in the preceding twelve months. We do not knowingly sell or share the personal information of consumers under sixteen years of age.

f. Use of Sensitive Personal Information

We use sensitive personal information only for purposes that the CCPA permits without separate opt-in or opt-out, namely to provide the Web Application's services as you have requested, to ensure the security and integrity of the Web Application, and to comply with law. We do not use sensitive personal information to infer characteristics about you.

g. Your Rights

If you are a California resident, you have the right to:

- **Know** what personal information we have collected about you, including the categories of information, the sources, the purposes for which it is used, and the categories of third parties to whom it has been disclosed.
- **Access** the specific pieces of personal information we have collected about you.
- **Correct** inaccurate personal information that we maintain about you.
- **Delete** personal information we have collected from you, subject to certain exceptions provided by law.
- **Not be discriminated against** for exercising any of these rights.

h. How to Exercise Your Rights

To exercise any of these rights, please contact us at info@ablelinktech.com or +1 719.592.0347. We will need to verify your identity before responding to your request, which may require you to confirm information already associated with your account.

You may also designate an authorized agent to make a request on your behalf. We may require the agent to provide proof of authorization and may require you to verify your own identity directly with us.

We will respond to verifiable requests within the timeframes required by California law. There is no charge to exercise these rights.

13. Users Outside the United States

The Web Application is hosted in the United States and is intended primarily for users in the United States. If you access the Web Application from outside the United States, you understand that your information will be transferred to, stored in, and processed in the United States.

14. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. Any changes will be posted in this document with the "Effective Date" updated. We encourage you to review this Privacy Policy periodically.

15. Contact Us

If you have any questions or concerns about this Privacy Policy or our data practices, please contact us at:

- info@ablelinktech.com
- +1 719.592.0347