



Staffbase Product-Specific Terms

These Product-Specific Terms are effective from 5 May 2023.

Customer's use of the specific Staffbase Services below is subject to these Product-Specific Terms and the service agreement entered into between Customer and Staffbase referencing these Product-Specific Terms (the "**Agreement**"). Terms not expressly defined here have the same meanings as in the Agreement.

Employee App-Specific Terms

Scope of Use (numerical limit on invited Authorized Users). Customer can invite Authorized Users to create an account for Customer's Employee App. Numerical limits related to Employee App are based on the number of invited Authorized Users. The Order Form specifies the number of Authorized Users that Customer may invite. If Customer invites more Authorized Users than specified in the applicable Order Form, Customer exceeds its Scope of Use. Invited Authorized User counts are based on the data available in the Services. Deactivated users (previously invited Authorized Users that accepted the invitations, registered, and then have been deactivated in the relevant Service) are not counted towards the total of invited Authorized Users. For Customers using SSO integrations, including SCIM, SAML, or OIDC, without a regular sync with the Services of the full invited user base, the ability to log in and register for the Services through the integration is counted as an "invitation".

Employee App Specific License. For Employee Apps, the right and license granted in Agreement, subject to the same conditions, further includes: **(i)** for Authorized Users of the Employee App or those that download the Employee App, a worldwide (other than in a country or jurisdiction where downloading or using the Employee App is prohibited by the App Store's terms), non-exclusive, non-transferrable, and non-sublicensable right and license during the Subscription Term to install and use the Employee App; and **(ii)** for Customer, the right and license during the Subscription Term to distribute the Employee App to Authorized Users and the limited right to sublicense distribution through Apple's App Store, the Google Play Store, or another eligible app store ("**App Store**") (if applicable). Upon any expiration or termination of a Subscription Term, Customer's license to use and distribute any software related to the Employee App terminates immediately.

Customer's App Store Account. When Customer distributes the Employee App via an App Store, Customer may be required to sign up for a specific App Store account. Customer is responsible for complying with any relevant terms of service and requirements of any App Stores related to their App Store account and Customer will maintain the functionality of their App Store account. Where Staffbase supports Customer in distributing or managing the Employee App on Customer's behalf, Customer will ensure Staffbase has appropriate access to Customer's App Store account.

App Store Distribution Support. Staffbase will use reasonable efforts to support Customer in its App Store submissions, such as providing any needed documentation or information about the Employee App that is available to Staffbase. Unless otherwise agreed in writing, Customer is responsible for the distribution and use of their Employee App in the relevant App Store(s). When Staffbase, on Customer's instructions and behalf, distributes the Employee App via Staffbase's own App Store account, Customer remains responsible for the distribution and use of the Employee App as set out in the Agreement and Customer will provide Staffbase with all required information necessary for Staffbase to distribute and maintain the Employee App in the App Store (including Customer's Employee App privacy policy and any other information about personal data processing required by the relevant App Store).

Staffbase Updates. From time-to-time Staffbase may update functionality of the Employee App to take into account relevant App Store terms of service and requirements.



Product-Specific Terms

New Employee App Versions. From time-to-time, Staffbase may provide new versions of the Employee App to Customer. Customer may lose access to the Employee App if the Employee App is not updated to a newer app version in line with the Documentation. Customer agrees that: **(i)** if Customer distributes the Employee App via App Stores, Customer will promptly submit updates to the App Store (and within 48 hours for emergency security-related updates), and Customer must use commercially reasonable efforts to encourage its Authorized Users to update the Employee App; **(ii)** if Customer distributes via a channel Customer controls (such as Mobile Device Management, a company internal app store, or a self-hosted download page), Customer will promptly update the Employee App on the devices it manages (and within 48 hours for emergency security-related updates); **(iii)** if Customer distributes via a download page, Customer will, where relevant, promptly update the Employee App on the relevant download page (and within 48 hours for emergency security-related updates), and Customer must use commercially reasonable efforts to encourage its Authorized Users to update the Employee App; and **(iv)** if Staffbase manages the Employee App on Customer's behalf, Customer will promptly provide Staffbase with the necessary documentation or provide Staffbase access to Customer's account to update the Employee App. If reasonably required for the security of the Staffbase Service, Staffbase may disable older versions of the Employee App from accessing the Staffbase Service.

Branding of the Employee App. For certain plans, Staffbase makes available the ability to customize the Employee App with branding by the Customer. Logos and any branding of the Employee App are "Customer Content" as defined in the Agreement. Customer exclusively owns any goodwill generated through the use by Staffbase of its branding (including any trademarks) under the Agreement. Any changes to the branding of the Employee App after the initial selection has been made may be subject to additional fees, to be agreed between Customer and Staffbase in an Order Form.

Employee App Privacy Policy. App Store(s) may require Customer to have a privacy policy in place when submitting the Employee App to the relevant App Store(s). Customer is responsible for creating their own privacy policy. Staffbase will use reasonable efforts to support Customer in creating the privacy policy, such as providing any needed documentation or information about the functionality of the Employee App that is available to Staffbase. Customer is not allowed to use, copy, or refer to a privacy policy created by Staffbase.

Employee App Privacy Labels. The App Store(s) may require Customer to specify what user data is collected and shared by the Employee App, for example via the creation of so called "privacy labels". Customer is responsible for answering any questions about the relevant Employee App data processing activities and for creating the appropriate privacy labels in accordance with the App Store(s)' terms of service and requirements. Staffbase will use reasonable efforts to support Customer, such as providing any needed documentation or information about the functionality of the Employee App that is available to Staffbase.

Front Door Intranet-Specific Terms

Scope of Use (numerical limits on invited Authorized Users). Customer can invite Authorized Users to create an account for Customer's Front Door Intranet. Numerical limits related to Front Door Intranet are based on the number of invited Authorized Users. The Order Form specifies the number of Authorized Users Customer may invite. If Customer invites more Authorized Users than specified in the applicable Order Form, Customer exceeds its Scope of Use. Invited Authorized User counts are based on the data available in the Services. Deactivated users (previously invited Authorized Users that accepted the invitations, registered, and then have been deactivated in the relevant Service) are not counted towards the total of invited Authorized Users. For Customers using SSO integrations, including SCIM, SAML, or OIDC, without a regular sync with the Services of the full invited user base, the ability to log in and register for the Services through the integration is counted as an "invitation".

Custom Domains or Subdomains. Any Customer-provided names for any custom subdomains or custom domains related to their Front Door Intranet are "Customer Content" as defined in the Agreement. Customer exclusively owns any goodwill generated through the use by Staffbase of its



Product-Specific Terms

branding within custom subdomains or for custom domains (including any trademarks) under the Agreement. Any changes to custom domains or subdomains after the initial selection has been made may be subject to additional fees, to be agreed between Customer and Staffbase in an Order Form.

Employee Email-Specific Terms

Scope of Use (Numerical limits on Email Recipients). The numerical limits for Employee Email are based on the number of unique recipients that receive emails sent by Customer using the Services (“Email Recipients”). The numerical limits are specified on the Order Form and calculated based on the number of unique individual email recipients reached via Employee Email during an applicable Subscription Term. If Customer communicates to more Email Recipients than specified in the applicable Order Form, Customer exceeds its Scope of Use.

Staffbase Email for Outlook or Gmail Specific License. For Staffbase Email for Outlook or Gmail, the right and license granted in Agreement, subject to the same conditions, further includes: **(i)** for those that download the Outlook add-on or Gmail extension, a worldwide, non-exclusive, non-transferrable, and non-sublicensable right and license during the Subscription Term to install and use the Outlook add-on or Gmail extension; and **(ii)** for Customer, the right and license during the Subscription Term to distribute the Outlook add-on or Gmail extension, subject to Customer’s compliance with any applicable terms and conditions of Outlook or Gmail. Upon any expiration or termination of a Subscription Term, Customer’s license to use and distribute any software related to the Outlook add-on or Gmail extension terminates immediately.

Email tracking and analytics. Employee Email comes with its own analytic features that enable Customer to analyze the success of email newsletters via advanced analytics and reports. To track email newsletter engagement, technologies like pixels and cookies may be used. Customer must determine whether Customer’s use of these technologies is permitted under applicable law.

Customer’s compliance with applicable law. Customer agrees to use Employee Email solely for Customer’s internal communications and is responsible for any required consents, authorizations, or disclosures to Email Recipients as required by applicable law.

Customer’s obligations to mitigate risks related to spam complaints. Email Recipients may have the option to mark Customer’s emails as “spam”. Customer understands that the Services may be impacted by the amount of spam complaints related to Customer’s emails. Customer agrees that Staffbase may monitor spam complaints submitted by Email Recipients. Customer also agrees that Staffbase may take the necessary measures to protect its own interests and to prevent any harm or liability to Staffbase’s customers or other third parties. These measures may include suspension of access to the Service or termination of the Agreement, in accordance with the Agreement. Customer will promptly follow Staffbase’s instructions to mitigate any risks related to spam complaints in relation to Customer’s use of the Services.

Customer Content. Customer acknowledges and agrees that any Customer Content that is part of an email newsletter, including media files, will be visible to each Email Recipient, and may be forwarded by an Email Recipient. Any additional access restrictions activated or implemented by Customer in relation to other Services are not applicable to media files contained in email newsletters sent via Employee Email. Customer is solely responsible for the configuration of Email Recipient lists and Staffbase is not responsible for access to, or use of, email newsletters outside of the Services, such as email newsletters forwarded by Email Recipients.

Communications Control-Specific Terms

Scope of Use (numerical limits on Authorized Users). The Order Form specifies the number of Authorized Users for Communications Control.

Storage space. The available storage space for Communications Control is subject to limitations, as specified in the Documentation and/or referenced exhibits. Customer may be able to purchase



Product-Specific Terms

additional storage space that is limited to Communications Control. Customer agrees that Staffbase will make available the additional storage space as specified on the Order Form.

Customer's social media accounts. Staffbase allows Customer to send communication via various external channels, including Customer's social media accounts. Customer must identify which third-party terms apply when connecting the Communications Control Platform to the relevant Customer's social media account. Customer agrees that it will comply with any applicable guidelines, terms and conditions, or policies of the relevant social media platform when using the Communications Control Platform. When Customer has connected their social media accounts to the Communication Control Platform, Staffbase may process Personal Data (as defined in the DPA) of individuals who engage with Customer via Customer's social media accounts ("**Social Media Contacts**"). Customer understands that it is responsible for any required consents, authorizations, and disclosures when processing Personal Data of Social Media Contacts in relation to the Staffbase Services and when communicating with Social Media Contacts via the Staffbase Services, as required by applicable laws and applicable social media terms and conditions. Staffbase cannot be held responsible if a social media platform provider changes their API interface that results in a complete or partial use restriction of the relevant connection between the social media platform and the Communications Control Platform. The individual social media platforms and any other external channels (not developed by Staffbase) that are connected to the Communications Control Platform by or on behalf of Customer are "Third-Party Services" as defined in the Agreement.

Security. Notwithstanding any other provision in the Agreement, the applicable technical and organizational measures in relation to Communications Control are currently available at: <https://dirico.io/en/trust/> and <https://staffbase.com/en/legal/dpa/>. Customer acknowledges that the technical and organizational measures applicable to Communications Control may differ from the technical and organizational measures that apply to other Services and that are described on Staffbase's Security webpage, currently available at <https://staffbase.com/en/security/>.

Updated Definitions. When Customer uses Communications Control, the following definition, as defined in the Agreement, will include the following:

"Documentation" includes the documentation available at: <https://dirico.io/en/support/> and <https://content.dirico.io/en/function-description>.