



## Privacy Policy

***Last updated: 10<sup>th</sup> May 2018***

***Effective from: 10<sup>th</sup> May 2018***

Thrive IT Ltd. is committed to protecting the privacy of all of our customers. This privacy policy applies to all data collected and stored by Thrive IT Ltd. through our website and your use and administration of TeamTrack services ("The Service," as further defined below). It does not apply to the privacy policies of other linked or integrated services, our data storage providers or **third-party sub-processors**.

### Definitions we use in this document

- **"The Service"** means our TeamTrack software, which is accessed online through a web browser, or by using our mobile application (App). Access is provided through a unique username/password/Microsoft account.
- **"your Organisation"** means your company, charity or other type of organisation that has opened a TeamTrack account. In the relationship between us, your Organisation should be considered the Data Controller as defined within the context of the General Data Protection Regulation (GDPR) and UK data protection law.
- **"us", "we" and "our"** refer to Thrive IT Ltd. In the relationship between us, Thrive IT Ltd should be considered the Data Processor as defined within the context of the General Data Protection Regulation (GDPR) and UK data protection law.
- **"you"** means you, the person who accesses The Service on behalf of your Organisation. This may include others within your Organisation to whom you choose to grant user access to The Service.

### How do we use your information?

**When using our website**, the personal information we collect might include your IP address, what pages you may have visited and when you accessed them. This information helps us to tailor the website to your interests. Full details on our use of cookies can be found in our **Cookie Policy**.

**When you first sign up for a trial of The Service**, you are required to provide basic contact information to enable us to create your trial account to access The Service. The contact details you provide are used solely to communicate with you throughout your trial experience. At the end of the trial period, if you wish to continue to access The Service on a paid subscription basis, those same contact details are retained.

If the account contact person changes within your organisation at any time please contact our support team.

We comply with our obligations under the GDPR by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

In the interests of transparency, we've set out the specific information we may collect about you when you sign up for a TeamTrack account and how we keep your information confidential and secure.

## What is our lawful basis for using your information?

We have various scenarios under which we may use your information, and for each have identified a lawful basis, as described below:

- **Contract** applies:
  - If you have subscribed to use The Service (see our related **Terms of Service**), processing is necessary to perform and manage the contract.
- **Legitimate interest** applies:
  - Where the contract between us has ended – either because you have closed/ ended your trial of TeamTrack or you have cancelled your subscription to The Service. We will opt you out of all communication and not contact you after the contract has ended; unless you contact us or have requested we contact you at a later date. However, we will retain your contract contact details for internal statistical and reporting purposes.
  - Where we need to communicate with you about:
    - A technical issue or bug within The Service that affects you,
    - Any security-related matter,
    - New features and functionality added to The Service, or changes to existing,
  - For good governance and accounting.
- **Legal obligation** applies:
  - When you exercise your rights under data protection law and related disclosures.
  - For maintaining and reporting financial accounting information for up to 6 years from the end of the tax year in which a financial transaction was processed.
- **Consent** applies:
  - Where you have voluntarily subscribed to the TeamTrack emailing list and explicitly consented to receiving our emails. You can unsubscribe from this list at any time using the unsubscribe link in the footer of those emails.

## Sharing your information

The information we hold about you will be treated as strictly confidential and we will not disclose any information, personal or otherwise, outside of Thrive IT Ltd. at any time, except as you direct or unless required by law. If compelled to disclose any information to a third party, we will use notify you in advance of a disclosure unless legally prohibited.

Payment Data (if payment by Direct Debit only) will be shared with third parties for purposes of fraud prevention or to process payment transactions only, as further described in this statement.

## How secure is your information?

We take security very seriously and will do everything we can to keep your information safe.

### Data Location

The Service and your data is stored within the Google Cloud platform within state-of-the-art data centres in the UK. For security and compliance information for the Google Cloud, please visit:

<https://cloud.google.com/security/> and <https://cloud.google.com/security/gdpr/>

Account contact and initial data may be stored within the Google Cloud or Microsoft Cloud as part of Microsoft's Office 365 services. For security and compliance information for the Microsoft Cloud, please visit: <https://www.microsoft.com/en-us/TrustCenter/Security/office365-security> and <https://www.microsoft.com/en-us/TrustCenter/CloudServices/office365/GDPR>

## Data Encryption

The Google Cloud platform, which hosts The Service, encrypts all data at rest by default. TeamTrack benefits from world-class encryption on the Google Cloud platform and data is automatically encrypted prior to being written to disk.

## Secure Data Access

TeamTrack data can only be accessed through the TeamTrack website or application, its API components or through access secured using secure encryption keys from pre-defined locations. All web browser sessions are secured with SSL certificates, rated A+ by Qualys, a global leading provider of information security and compliance solutions (10<sup>th</sup> May 2018).

**For further information on how we secure your information, please read our Security Policy.**

## How long do we keep your information?

We keep data in accordance with the guidance set out by the GDPR. We endeavour to maintain only data that is relevant, accurate and up to date. We have internal processes to periodically review the data we hold and delete data that is no longer relevant to our purpose for processing.

## Your rights and your information

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data: -

- **Access to your information:** You have the right to request a copy of the personal information about you that we hold.
- **Correcting your information:** We want to make sure that your personal information is accurate, complete and up to date and you may ask us to correct any personal information about you that you believe does not meet these standards.
- **Deletion of your information:** You have the right to ask us to delete personal information about you where:
  - you consider that we no longer require the information for the purposes for which it was obtained or that we no longer need to retain it in accordance with our statutory obligations;
  - you have validly objected to our use of your personal information - see 'Objecting to how we may use your information' below;
  - our use of your personal information is contrary to law or our other legal obligations.
- **Objecting to how we may use your information:** Where we use your personal information to perform tasks carried out in the public interest then, if you ask us to, we will stop using that personal information unless there are overriding legitimate grounds to continue.
- **Restricting how we may use your information:** In some cases, you may ask us to restrict how we use your personal information. This right might apply, for example, where we are checking the accuracy of personal information about you that we hold or assessing the validity of any objection you have made to our use of your information. The right might also apply where there is no longer a basis for using your personal information but you do not want us to delete the data. Where this right is validly exercised, we

may only use the relevant personal information with your consent, for legal claims or where there are other public interest grounds to do so.

- **Withdrawing consent using your information:** Where we use your personal information with your consent you may withdraw that consent at any time, and we will stop using your personal information for the purpose(s) for which consent was given. Please contact us if you wish to exercise any of these rights.
- **Lodging a complaint:** If you feel we have used your information incorrectly or without lawful basis, or you dispute our lawful basis, you have the right to lodge a complaint with the Information Commissioner's Office (ICO).

## Further processing

If we wish to use your information for a new purpose, not covered by this Privacy Policy, then we will provide you with a new notice explaining the new use prior to starting the processing and setting out the relevant purposes and legal basis for processing. Where and whenever necessary, we will seek your prior consent to the new processing.

## Our contact details

Requests for personal data should be made in writing to the address below or via email to [security@thrivewithus.co.uk](mailto:security@thrivewithus.co.uk). If you have questions about Thrive IT Ltd.'s privacy and security commitments please contact our support team.

Address: Thrive IT Ltd. 88 Brighton Road, Reading, Berkshire, RG6 1PS

Office Telephone: +44 (0)118 336 8326

THRIVE IT LTD. is a limited company registered in England and Wales, company number 10220836.

## Data collection disclosure

### Information we may collect about you/your organisation    What we use this information for

Organisation name	Used to create an account for The Service for your named organisation.
Organisation website	Used by us to help verify the existence of your organisation when a trial account is opened for The Service. Your organisation's domain name is also used to match support emails received from your organisation's domain name to your account.
Account contact first and last name	Each organisation will designate a named individual who will serve as our point of contact for matters relating to The Service. The account contact will also be our initial billing contact and data protection contact; however, you can update any of these at any time by contacting our support team.

Account contact email address	An email address is required in order to communicate with you about your account and account-related matters. Communications will also include periodic updates about new features and functionality, and to confirm changes requested to your account.
Account contact telephone number	Either a landline or mobile/cell number is required to contact you in case there is an account issue.
Account contact username	Used to create the first administrator account for you to access and setup The Service parameters.

**Other information we may derive or obtain**

Job title within your Organisation	This may be stated on your organisation's website, in your email signature, or where you have made this known to us. It's helpful to know if we are dealing with an organisation's director, an operational/office admin, a finance admin or someone with another role within your organisation.
Your organisation address, including postcode/zip code and country	This may be taken from your website, or you may provide this to us directly. This is primarily used to correctly configure your account.
Organisation type	We may produce internal reporting about the different types of organisations in our customer base.
Organisation 'known by' names	Where your organisation is known by more than one name, or by an abbreviation of your organisation name, we'll note these to help us better match email support requests to the correct customer account.

**Other information we maintain about your organisation**

Billing information	We maintain a financial history audit trail of invoices raised and payments made for The Service, including payment method, and overdue and unpaid accounts.
Statistics about your account	We maintain a record of the modules on your account and statistical information about module usage. This is used to calculate your monthly billing and statistical reporting.
Third-party integrations	We maintain a record of the third-party integrations that you've completed for your account.

## Payment Data

Payment data (if paying by Direct Debit only) is the information that you provide providing payment for The Service. This may include your name, billing address, account number and other financial data.

Payment data is used to complete transactions. In support of these uses, Thrive IT Ltd. may share your Payment Data with banks and other entities that process payment transactions or other financial services, for payment processing and fraud prevention.

## Support Data

Support data is the information we collect when you submit a support request. This may include any of the following: customer first and last name, customer job title, customer email address and customer contact phone number.

Support may be provided through phone or e-mail. On occasion, if required and with your express permission, we may use temporary 'Remote Access' software to assist you. We manage support data in the same way as we manage your information, as described in this privacy statement. Additionally, we use it to resolve your support incident and for internal training purposes.

## Cookies & Similar Technologies

The Service use "cookies", small text files placed on a device's hard disk by a web server. Most web browsers automatically accept cookies and usage of The Service requires this to be active. Cookie data is sent to the server and is used for the following purposes:

- Storing user preferences and settings.
- Sign-in and authentication.

The Service also uses "LocalStorage" to store additional user preferences and settings. This data remains on the local device at all times and is not transmitted to our servers.

We do not use analytics or data processing services in The Service.

## Security Incidents

If we become aware of any unlawful access to any data, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), we will: (a) notify you of the Security Incident; (b) investigate the Security Incident and provide you with information about the Security Incident; and (c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

You agree that:

- An unsuccessful Security Incident will not be subject to this section. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data. This may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents.
- Our obligation to report or respond to a Security Incident under this section is not and will not be construed as an acknowledgement by Thrive IT Ltd. of any fault or liability with respect to the Security Incident.
- Notification of a Security Incident, if any, will be delivered to one or more of your administrators by any means we select, including via email. It is your sole responsibility to ensure your administrators maintain accurate contact information at all times.

## Other Information

### Testing & Development Environments

All data used within our test and development environments is anonymised and contains no personal information.

### Microsoft Office 365 / SharePoint Online or Google Drive File Storage Integration

The optional file storage services use the Microsoft Graph API or Google Drive API to help store your project and event files. A folder structure is automatically created in the relevant online file storage service, based on the criteria you specify within TeamTrack. Documents generated in TeamTrack are then optionally stored in the relevant online file storage service based on project and event references. TeamTrack also provides direct links to folders within this structure. TeamTrack does not access or store user data provided by the third-party file storage service except to maintain a login by retrieving access tokens. TeamTrack does not store any documents from the online file storage service.

## Changes to the TeamTrack Privacy Policy

We will occasionally update this privacy policy to reflect changes in The Service. When we post changes to this statement, we will revise the "last updated" date at the top of the statement. If there are material changes to this statement or in how Thrive IT Ltd. will use or store your information, we will notify you by either posting a notice of such changes before they take effect, or by direct notification. We encourage you to periodically review this privacy statement to learn how Thrive IT Ltd. is protecting your information.