



TeamTrack

Privacy Policy

Last updated: 11th May 2026

1 BACKGROUND

1.1 This notice (**Privacy Notice**) tells you how we look after your personal data when you visit our website, at www.teamtrack.uk (**Website**), or when you use our system TeamTrack (**Service**), a cloud-based team and event management system developed and provided by Thrive IT Ltd. The Service is delivered as a hosted software-as-a-service (SaaS) application and is accessed online through a supported web browser or via the TeamTrack mobile applications. The Service is made available on an “as is” and “as available” basis.

The Service provides functionality enabling authorised users to manage team schedules and event planning, including assigning personnel and monitoring availability; track non-working days, holiday, leave, absences and working hours; record and maintain team and resource information such as skills, qualifications and contact details; generate and export documents and call sheets containing detailed event information; and access calendar data on mobile devices and through personal calendar feeds.

The Service may also include administrative tools for user management, role-based permissions, reporting and organisational configuration. Additional functionality may be made available through optional modules, subject to the applicable subscription and fees.

The Service is provided on a subscription basis and is intended for organisational and business use unless otherwise agreed in writing, where you are a prospective customer of our business, or where you are another type of business contact, such as a supplier or service provider to our business.

1.2 This notice sets out what information we collect about you, what we use it for and whom we share it with. It also explains your rights under data protection laws and what to do if you have any concerns about your personal data.

1.3 We may sometimes need to update this Privacy Notice, to reflect any changes to the way our services are provided or to comply with new business practices or legal requirements. You should check this Privacy Notice regularly to see whether any changes have occurred.

2 WHO WE ARE AND OTHER IMPORTANT INFORMATION

2.1 We are THRIVE IT LTD. trading as TeamTrack, registered in England and Wales with company number 10220836 with our registered address at Thornhill Road, Stockport, SK4 3HJ (**we, us or our**).

2.2 For all visitors to our Website and for users who purchase our services through an organisation, we are the **controller** of your information (which means we decide what information we collect and how it is used).

2.3 We are registered with the Information Commissioner’s Office (ICO), the UK regulator for data protection matters, under number ZA281340.

3 CONTACT DETAILS

3.1 If you have any questions about this Privacy Notice or the way that we use information, please get in touch using the following details:

Email address: support@teamtrack.uk

4 THE INFORMATION WE COLLECT ABOUT YOU

4.1 **Personal data** means any information which does (or could be used to) identify a living person. We have grouped together the types of personal data that we collect, and where we receive it from, below.

4.2 Type of personal data:

- **Identity Data:** your first and last name or title.
- **Contact Data:** your email address, telephone numbers and address.
- **Technical Data:** internet protocol (IP) address, browser type and version, time zone setting and generic location, operating system and platform on the devices you use to access our systems.
- **Usage Data:** information about how you use our systems.
- **Feedback:** information and responses you provide when completing surveys and questionnaires.
- **Photo and Image Data:** profile picture, images, videos and audio.
- **Profile Data:** email address, password, username, communication logs, audit trail of systems used and documents accessed and downloaded.
- **Marketing and Communication Data:** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

4.3 Please note that we do not collect or store any payment card details or similar financial information relating to your method of payment. All payment information is provided directly to GoCardless, which acts as our third-party payment processor and processes payments on our behalf. We receive and process only limited information relating to the amount, status and timing of payments made.

5 THIRD-PARTY SERVICE PROVIDERS AND SUB-PROCESSORS

5.1 In providing The Service, we may share personal data with carefully selected third-party service providers and sub-processors who assist us in delivering, securing, supporting and improving The Service.

5.2 These providers may include:

- cloud hosting and infrastructure providers;
- payment processing providers;
- customer support and ticketing providers;
- email and communications providers;
- analytics and monitoring providers; and
- optional third-party integration providers enabled by your Organisation.

5.3 Depending on your Organisation's use of The Service, these providers may process:

- user account information;
- contact details;
- authentication and login information;
- uploaded files and attachments;
- scheduling and event data;
- support communications;
- billing and payment information;
- identity verification information; and
- technical and usage data.

5.4 Certain optional integrations within The Service are enabled directly by your Organisation. Where such integrations are enabled, your Organisation authorises us to engage the relevant third-party provider for the purpose of delivering that functionality.

5.5 We maintain a current list of our third-party sub-processors, including information regarding their role and processing activities, which is available on request or via our website.

5.6 All third-party providers and sub-processors engaged by us are subject to contractual obligations requiring appropriate confidentiality, security and data protection measures in accordance with applicable UK and EU data protection laws.

6 SPECIAL CATEGORY AND SENSITIVE PERSONAL DATA

6.1 Depending on how your Organisation uses The Service, personal data uploaded or stored within

The Service may include sensitive or confidential information.

6.2 This may include:

- passport information and passport images;
- driving licence information and driving licence images;
- financial and banking information;
- employee absence or leave information;
- contact details;
- uploaded documents and attachments; and
- other information uploaded by authorised users of your Organisation.

6.3 Thrive IT Ltd. does not determine the purpose or lawful basis for processing personal data uploaded to The Service by your Organisation. Your Organisation remains responsible for ensuring that it has an appropriate lawful basis and any necessary permissions or notices required under applicable data protection law.

6.4 We process such information solely for the purpose of providing, maintaining, securing and supporting The Service in accordance with our contractual obligations to your Organisation.

7 INTERNATIONAL TRANSFERS

7.1 Hosting services for The Service are provided primarily within United Kingdom data centres.

Certain backup, support, infrastructure and sub-processing services may involve processing or storage within the United Kingdom, European Economic Area (EEA) or other jurisdictions.

7.2 Where personal data is transferred outside the United Kingdom or EEA, we ensure that appropriate safeguards are implemented in accordance with applicable data protection law.

7.3 Such safeguards may include:

- Standard Contractual Clauses approved by the European Commission;
- the UK International Data Transfer Addendum;
- adequacy regulations or decisions; and
- contractual confidentiality and security obligations with relevant providers.

7.4 Further information regarding international transfers and sub-processors may be obtained by contacting us using the contact details set out in this Privacy Notice.

8 TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

8.1 We implement appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

8.2 These measures include, where appropriate:

- encryption of data in transit using HTTPS/TLS;
- encryption of stored data where supported by the underlying infrastructure;
- role-based access controls and authentication mechanisms;
- multi-factor authentication for administrative access where applicable;
- infrastructure and network security controls;
- audit logging and monitoring;
- regular security review and testing;
- backup and disaster recovery processes;
- staff confidentiality obligations; and
- incident response and breach management procedures.

8.3 The Service is hosted using cloud infrastructure provided by trusted third-party providers, including Google Cloud services hosted primarily within UK regions.

8.4 Access to customer data is restricted to authorised personnel who require access for operational, support, security or legal purposes.

9 OPTIONAL THIRD-PARTY INTEGRATIONS

9.1 The Service may provide optional integrations with third-party platforms and services, including Microsoft Office 365, Google services and email delivery providers.

9.2 These integrations are enabled and configured by your Organisation and may require the exchange of certain information between The Service and the relevant third-party provider.

9.3 Depending on the integration enabled, this may include:

- authentication information;
- access tokens;
- linked file and folder metadata;

- email delivery information; and
- user account identifiers.

9.4 We only access and process information required to provide the requested integration functionality.

9.5 Use of optional integrations constitutes authorisation for us to engage the relevant third-party provider in connection with that functionality.

10 HOW WE USE YOUR INFORMATION

10.1 We are required to identify a legal justification (also known as a lawful basis) for collecting and using your personal data. There are six legal justifications which organisations can rely on. The most relevant of these to us are where we use your personal data to:

- fulfil our **contract** with you;
- comply with a **legal obligation** that we have.

10.2 Below is set out the lawful basis we rely on when we use your personal data. If we intend to use your personal data for a new reason that is not listed below, we will update our Privacy Notice.

10.2.1 Contract

- To administrate or perform our contract with you.
- To process your payment information in connection with any contract we have with you.
- To send you updates about the services you have bought (e.g. confirmation of order, arrival time).

10.2.2 Legal Obligation

- Recording your preferences (e.g. marketing) to ensure that we comply with data protection laws.
- Where we send you information to comply with a legal obligation (e.g. where we send you information about your legal rights).
- Where we retain information to enable us to bring or defend legal claims.

10.3 Where we need to collect your personal data (for example, in order to fulfil a contract we have with you), failure to provide us with your personal data may mean that we are not able to provide you with the services. Where we do not have the information required about you to fulfil an order, we may have to cancel the service ordered.

10.4 We may anonymise the personal data we collect so that it can no longer be used to identify you and combine it with other anonymised information to create aggregated data. Such aggregated data is used for analytical and statistical purposes, including identifying trends and patterns in system usage.

Once data has been anonymised so that individuals are no longer identifiable, it is no longer considered personal data under applicable data protection legislation. Accordingly, data protection laws do not apply to aggregated data and the individual rights described in this Privacy Policy do not apply to such data.

11 WHO WE SHARE YOUR INFORMATION WITH

11.1 We share (or may share) your personal data with:

- **Our personnel:** our employees or contracted workers who have contracts containing confidentiality and data protection obligations.

11.2 If we were asked to provide personal data in response to a court order or legal request (e.g. from the police), we would seek legal advice before disclosing any information and carefully consider the impact on your rights when providing a response.

12 WHERE YOUR INFORMATION IS LOCATED OR TRANSFERRED TO

12.1 We store your personal data on our servers in the UK.

12.2 We will only transfer information outside of the UK or EEA where we have a valid legal mechanism in place (to make sure that your personal data is guaranteed a level of protection, regardless of where in the world it is located, e.g. by using contracts approved by the ICO or the UK Secretary of State).

12.3 If you access our Website or purchase our services whilst abroad then your personal data may be stored on servers located in the same country as you or your organisation.

13 HOW WE KEEP YOUR INFORMATION SAFE

13.1 We have implemented security measures to prevent your personal data from being accidentally or illegally lost, used or accessed by those who do not have permission. These measures include:

- access controls and user authentication (including multi-factor authentication);
- internal IT and network security;
- regular testing and review of our security measures;
- staff policies and training;
- incident and breach reporting processes;
- business continuity and disaster recovery processes.

13.2 If there is an incident which has affected your personal data and we are the controller, we will notify the regulator and keep you informed (where required under data protection law). Where we act as the processor for the affected personal data, we notify the controller and support them with investigating and responding to the incident.

13.3 If you notice any unusual activity on the Website, please contact us support@teamtrack.uk

14 HOW LONG WE KEEP YOUR INFORMATION

14.1 Where we act as the controller, we will only retain your personal data for as long as necessary to fulfil the purposes we collected it for.

14.2 To decide how long to keep personal data (also known as its retention period), we consider the volume, nature, and sensitivity of the personal data, the potential risk of harm to you if an incident were to happen, whether we require the personal data to achieve the purposes we have identified or whether we can achieve those purposes through other means (e.g. by using aggregated data instead), and any applicable legal requirements (e.g. minimum accounting records for HM Revenue & Customs).

14.3 We may keep Identity Data, Contact Data and certain other data (specifically, any exchanges between us by email or any other means) for up to seven years after the end of our contractual relationship with you.

14.4 If you browse our Website, we keep personal data collected through our analytics tools for only as long as necessary to fulfil the purposes we collected it for.

14.5 If you have asked for information from us or you have subscribed to our mailing list, we keep your details until you ask us to stop contacting you.

15 YOUR LEGAL RIGHTS

15.1 You have specific legal rights in relation to your personal data.

15.2 We can decide not to take any action in relation to a request where we have been unable to confirm your identity (this is one of our security processes to make sure we keep information safe) or if we feel the request is unfounded or excessive. Usually there is no cost for exercising your data protection rights, but we may charge a fee where we decide to proceed with a request that we believe is unfounded or excessive. If this happens we will always inform you in writing.

15.3 We will respond to your legal rights request without undue delay, but within one month of us receiving your request or confirming your identity (whichever is later). We may extend this deadline by two months if your request is complex or we have received multiple requests at once. If we need to extend the deadline, we will let you know and explain why we need the extension.

15.4 We do not respond directly to requests which relate to personal data for which we act as the processor. In this situation, we forward your request to the relevant controller and await their instruction before we take any action.

15.5 If you wish to make any of the right requests listed below, you can reach us at support@teamtrack.uk

15.6 Your rights include:

- **Access:** You must be told if your personal data is being used and you can ask for a copy of your personal data as well as information about how we are using it to make sure we are abiding by the law.
- **Correction:** You can ask us to correct your personal data if it is inaccurate or incomplete. We might need to verify the new information before we make any changes.
- **Deletion:** You can ask us to delete or remove your personal data if there is no good reason for us to continue holding it or if you have asked us to stop using it (see below). If we think there is a good reason to keep the information you have asked us to delete (e.g. to comply with regulatory requirements), we will let you know and explain our decision.
- **Restriction:** You can ask us to restrict how we use your personal data and temporarily limit the way we use it.
- **Objection:** You can object to us using your personal data if you want us to stop using it. If we think there is a good reason for us to keep using the information, we will let you know and explain our decision.
- **Portability:** You can ask us to send you or another organisation an electronic copy of your personal data.
- **Complaints:** If you are unhappy with the way we collect and use your personal data, you can complain to the ICO or another relevant supervisory body, but we hope that we can respond to your concerns before it reaches that stage. Please contact us at support@teamtrack.uk

16 WHEN WE SEND YOU MARKETING MESSAGES

16.7 We market our services to prospective and existing business customers; this is known as Business-to-Business Marketing (**B2B Marketing**). We may send marketing communications to their staff via work contact details. If you are a member of staff and do not wish to receive B2B Marketing, please let us know at support@teamtrack.uk

16.8 Opting out of marketing will not affect our processing of your personal data in relation to any order you have with us and where we are required to use your personal data to fulfil that order or provide you with certain information.

17 KEEPING THIS POLICY UP TO DATE

17.1 This policy shall be reviewed:

- at least annually;
- following significant changes to the TeamTrack platform or cloud infrastructure;
- following significant security incidents;
- following changes to applicable legislation or recognised security best practice.

17.2 The Company Directors are responsible for approving and maintaining this policy.

17.3 Material changes shall be communicated to all relevant personnel.