Data Breach Policy

Last updated and effective from: 2nd March 2026

1 ABOUT THIS POLICY

1.1 This policy applies to all members of staff: whether you have an employment contract with us or work for us in some other capacity (e.g. contractor, work experience), you must abide by this policy.

1.2 This policy applies to all personal data that is collected, stored, used or is accessible by our business: THRIVE IT LTD. trading as TeamTrack (with company number: 10220836) (**we**, **us** or **our**) use personal data when we conduct our business. Personal data is any information which does (or could be used to) identify a living person. It does not matter whether their information is kept digitally or in hard-copy, or whether it is in writing or some other format (e.g. CCTV footage, photographs).

1.3 Why we have this policy: this policy forms part of a suite of data protection policies which describe some of our organisational measures to protect personal data. This policy explains how to recognise when something has gone wrong (there has been a data breach) and what you should do next.

1.4 Who checks this policy is enforced: the Information Commissioner's Office (ICO) is the UK regulator and is responsible for checking that businesses comply with data protection law. Simon Bond is our Data Protection Officer and is responsible for advising and monitoring our data protection in our business. They advise senior management on data protection matters. Our senior management is responsible for making (and providing adequate resources to implement) any decisions, including whether to report a breach to the ICO.

1.5 How is this policy enforced: the ICO handles complaints and can fine businesses that do not fulfil their data protection obligations. Our employment (and equivalent) contracts require our staff to abide by this policy and we may conduct a disciplinary investigation where this policy has not been followed.

2 WHAT IS A DATA BREACH?

2.1 You must be able to confidently recognise a data breach: you have a responsibility to recognise where there has been a data breach and notify us about it as soon as possible. A data breach is a security incident in which personal data has been accidentally or illegally:

2.1.1 Destroyed: the information has been permanently deleted (if it is electronic) or it has been damaged beyond use (e.g. hard copy documents have been shredded or electronic files have been corrupted) and there is no copy or other version of the information.

2.1.2 Lost: there is no clear evidence that the information has been destroyed but it cannot be found even after extensive searches. Even if the information is later found, there has been a data breach (albeit one that has been resolved).

2.1.3 Changed: the information has been changed maliciously (e.g. changing bank account details so funds are redirected to an imposter) or by mistake (e.g. overwriting an address on a customer database).

2.1.4 Shared: it was accessed or used by someone who did not have permission. Information should only be shared, accessed and used by those who are authorised. This extends beyond malicious individuals (e.g. hackers committing cyber-attacks) and includes circumstances where information has been emailed to the wrong recipient or information has not been stored properly (e.g. disciplinary outcome letter found on a photocopier).

3 WHAT TO DO IF YOU SUSPECT THERE HAS BEEN A DATA BREACH

3.1 Let Company Directors know as soon as possible: we (as a business) have an obligation to record and investigate suspected data breaches within a strict deadline (72 hours, usually less if we use the information on behalf of other business customers). Do not wait to report a data breach, even if you are not sure whether it is real or not. It is always best to be cautious. You should report any suspected data breach by via email.

3.2 Provide as much detail as you can: the more information you can provide Company Directors, the better. Here are some examples of useful information:

- How did you discover the issue (e.g. a customer reported suspicious activity on their account)?
- What time did you discover the issue?
- Have you taken any action (e.g. recalled an email sent to the wrong recipient)?
- What types of information are at risk (e.g. contact details, payroll numbers, medical records)?
- Whose information is at risk (e.g. customer, staff)?
- What kind of risk does it create for that person (e.g. identity fraud, embarrassment,
- discrimination)?

3.3 Company Directors will decide whether to report the breach to the ICO: once you have notified Company Directors, you do not need to take any further action (unless you receive a specific instruction, e.g. reset your password). It is the responsibility of Company Directors to investigate your report and suggest next steps to Company Directors. Company Directors makes the decision about whether the incident should be reported to the ICO or any other action should be taken.

3.4 If you fail to report a breach or suspected breach: failure to comply with this policy puts you and the business at risk and is a very serious issue. You may be liable to disciplinary action if you fail to comply with this policy.

4 WHAT THE BUSINESS WILL DO IN THE EVENT OF A DATA BREACH

4.1 Containment: we will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data.

4.2 Recovery: we will identify ways to recover, correct or delete data. This may include contacting the police, e.g. where the breach involves stolen hardware or data.

4.3 Notify: depending on the circumstances of the breach, there are a number of parties that may need to be notified. This includes:

- the ICO (as mentioned above, where a breach is reportable to the ICO, this must be notified within 72 hours);
- individuals who either were or may be affected by the data breach;
- the police if we suspect criminal activity;
- our other business contacts who may be involved e.g. suppliers, website developers, external IT support;
- our insurance providers e.g. professional indemnity, cyber insurance.

4.4 Assess and record: we will record any breaches in our data breach register. In order to assess the seriousness (including whether an ICO notification is required), we will assess the data breach based on the following factors:

4.4.1 The potential harm to the rights and freedoms of data subjects: this is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage.

4.4.2 The volume of personal data: there should be a presumption to report the breach to the ICO where:

- a large volume of personal data is concerned; and
- there is a real risk of individuals suffering some harm.

It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.

4.4.3 The sensitivity of data: even if there is only a small amount of personal data involved, but it has the capability to cause those individuals harm (including financial or distress), then there should be a presumption to report to the ICO. This is most likely to be the case where the breach involves special category personal data. This

includes personal data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetic information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation. If the information is particularly sensitive, even a single record could trigger a report.

5 PREVENTING FUTURE BREACHES

5.1 **Prevention is always better than cure:** data security concerns may arise at any time and we encourage you to report any concerns you have to Company Directors. This helps us capture risks as they emerge, protect our company from personal data breaches, and keep our processes up-to-date and effective.

5.2 **Training:** the key to prevent data breaches is staff awareness, we provide regular training:

- at induction;
- when there is any change to the law, regulation or our policy;
- when significant new threats are identified;
- at regular intervals (e.g. yearly data protection training).

5.3 **Learning from experience:** once the personal data breach has been dealt with, in accordance with this plan, Company Directors will:

- establish what security measures were in place when the breach occurred;
- assess whether technical or organisational measures can be implemented to prevent the breach from happening again;
- consider whether there is adequate staff awareness of security issues and look to fill any gaps
- through training or tailored advice;
- consider whether it is necessary to conduct a privacy risk assessment;
- update the privacy risk register;
- debrief the team members following the investigation.

6 QUESTIONS ABOUT THIS POLICY

Questions regarding this policy should be directed to the Company Directors at:

support@teamtrack.uk

7 KEEPING THIS POLICY UP TO DATE

7.1 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.

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

7.3 Material changes shall be communicated to all relevant personnel.