Data Protection Policy

1. Aim and Scope of Policy

This policy applies to the processing of personal data in manual and electronic records kept by Thrive Tribe. It also covers Thrive Tribe's response to any data breach and other rights under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy should be read alongside Thrive Tribe's Privacy Statement (thethrivetribe.com/privacy).

This policy applies to the personal data of employees and learners; job applicants; existing and former employees; apprentices; volunteers; placement students; workers and self-employed contractors; and potential, existing and completed learners. These are referred to in this policy as relevant individuals.

2. Definitions

“Personal data” is information that relates to an identifiable person who can be directly or indirectly identified from that information — for example, a person's name, identification number, location, or online identifier. It can also include pseudonymised data.

“Special categories of personal data” is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for identification purposes).

“Criminal offence data” is data which relates to an individual's criminal convictions and offences.

“Data processing” is any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.

Thrive Tribe is committed to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate), is processed in line with UK GDPR and domestic law, and that all staff, associates and subcontractors conduct themselves in line with this policy. Where third parties process data on Thrive Tribe's behalf, Thrive Tribe will ensure that the third party takes appropriate measures to maintain this commitment. Thrive Tribe is accountable for the processing,

management, regulation, storage and retention of all personal data it holds, whether in manual records or on computer systems.

3. Types of Data Held

The following types of data may be held by Thrive Tribe, as appropriate, on relevant individuals:

- Name, address and phone numbers — for the individual and next of kin
- CVs and other information gathered during recruitment
- References from former employers
- National Insurance numbers
- Job title, job description and pay grade
- Conduct-related records, such as letters of concern or disciplinary proceedings
- Holiday records
- Internal performance information
- Medical or health information
- Sickness absence records
- Tax codes
- Terms and conditions of employment
- Training details and learner records

Relevant individuals should refer to Thrive Tribe's Privacy Statement for further information on the reasons for processing, the lawful bases relied upon, and data retention periods.

4. Data Protection Principles

All personal data obtained and held by Thrive Tribe will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- be kept accurate and up to date, with every reasonable effort made to rectify or erase inaccurate data without delay
- not be kept for longer than necessary for its given purpose

- be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical and organisational measures
- comply with the relevant UK GDPR procedures for the international transfer of personal data

5. Individuals' Rights

Personal data will be processed in recognition of individuals' data protection rights, including:

- the right to be informed
- the right of access
- the right to have inaccuracies corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict processing
- the right to data portability
- the right to object to processing
- the right to regulate automated decision-making and profiling

6. Procedures

Thrive Tribe has taken the following steps to protect the personal data of relevant individuals which it holds or has access to:

- responsibility for data processing and data protection compliance sits with the Director, who is accountable for reviewing and auditing data protection systems and procedures and for the effectiveness and integrity of the data held
- individuals are provided with information on their data protection rights, how their personal data is used, and how it is protected, including what action to take if they believe their data has been compromised
- staff, associates and subcontractors are given information and guidance to make them aware of the importance of protecting personal data, and how to treat information confidentially, in line with this policy and the Information Security Policy
- Thrive Tribe can account for all personal data it holds, where it comes from, and who it is or might be shared with

- risk assessments are carried out as part of ongoing review to identify vulnerabilities in personal data handling and processing, and to reduce the risk of mishandling or breaches
- where consent is relied upon as a lawful basis, Thrive Tribe recognises that consent must be freely given, specific, informed and unambiguous, and that individuals have the right to withdraw consent at any time
- Thrive Tribe has mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, in line with the Thrive Tribe Incident Response Plan, and is aware of its duty to notify the Information Commissioner's Office (ICO) of breaches likely to result in a risk to individuals

7. Access to Data (Subject Access Requests)

Relevant individuals have the right to be informed whether Thrive Tribe processes personal data relating to them, and to access the data Thrive Tribe holds about them. Requests are handled as follows:

- A request for access to personal data (a Subject Access Request) should be made to the Director
- Thrive Tribe will not charge for supplying data unless the request is manifestly unfounded, excessive or repetitive, or unless duplicate copies are requested for parties other than the individual making the request
- Thrive Tribe will respond without delay, and in any event within one month as a maximum, extendable by a further two months where a request is complex or numerous

Relevant individuals should inform Thrive Tribe immediately if they believe their data is inaccurate, whether identified through a subject access request or otherwise, and Thrive Tribe will take prompt steps to rectify it.

8. Learner Records and Achievements

Learner records and details of achievement are completed on the day of attainment and stored securely in Google Drive, which is protected by the access controls, encryption and multi-factor authentication set out in the Thrive Tribe Information Security Policy and Password Policy.

- Any electronic documents sent in relation to learner records and achievements are password protected
- Any paper-based information relating to learner records is stored in a locked filing cabinet, with keys available only to those who require access

9. Data Disclosures

Thrive Tribe may be required to disclose certain data to third parties in limited circumstances, including:

- relevant funding bodies
- any employee benefits operated by third parties
- where reasonable adjustments are required to support a disabled individual
- individuals' health data, to comply with health and safety or occupational health obligations
- for Statutory Sick Pay purposes
- HR management and administration, to consider how an individual's health affects their ability to do their job
- the operation of any employee insurance policies or pension plans

These disclosures are only made when strictly necessary for the stated purpose.

10. Data Security

Thrive Tribe adopts procedures designed to maintain the security of personal data when it is stored and transmitted, in line with the Thrive Tribe Information Security Policy and Password Policy. In addition, all staff, associates and subcontractors must:

- ensure that all files or written information of a confidential nature are stored securely and only accessed by those who have a need and a right to access them
- ensure that confidential files or written information are not left where they can be read by unauthorised people
- check regularly on the accuracy of data being entered into computer systems
- use their own credentials to access business systems and never share passwords with others
- use automatic screen locking to ensure personal data is not left visible on screen when a device is not in use

Personal data is stored and shared only through Google Drive and GoHighLevel, in line with the Thrive Tribe Information Security Policy; it is not stored on removable media such as USB sticks, in line with the Removable Media provisions of that policy.

Failure to follow Thrive Tribe's data security rules may be dealt with under Thrive Tribe's disciplinary procedure, with sanctions appropriate to the severity of the failure.

11. Cyber Attack and Security Incidents

In the unlikely event of a cyber attack or other information security incident affecting personal data, Thrive Tribe will follow its Incident Response Plan, including taking affected systems offline where necessary and changing passwords immediately. If a cyber attack occurs during a live or controlled assessment, the assessment will stop immediately and be treated as void; a new date will be issued to learners to retake the assessment and maintain examination integrity.

Thrive Tribe will inform all relevant contract owners and awarding bodies of the event immediately, along with the steps taken to address it, as well as the ICO where required.

12. International Data Transfers

Thrive Tribe does not transfer personal data to any recipients outside of the UK or European Economic Area (EEA).

13. Breach Notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner's Office (ICO) within 72 hours of Thrive Tribe becoming aware of it, and may be reported in more than one instalment where full details are not yet available. Individuals will be informed directly where a breach is likely to result in a high risk to their rights and freedoms. Where a breach is sufficient to warrant notification to the public, Thrive Tribe will do so without undue delay. This is in line with the Thrive Tribe Incident Response Plan.

14. Training

- New staff, associates and subcontractors are made aware of this policy as part of their induction
- All staff receive guidance covering basic confidentiality and data protection principles, and the action to take upon identifying a potential data breach
- The Director, as the person responsible for data protection compliance, keeps their own knowledge of UK GDPR requirements up to date
- Staff who use Thrive Tribe's computer systems are made aware of how to protect individuals' data, maintain data security, and understand the consequences of any lapse or breach of this policy

15. Records

Thrive Tribe keeps a record of its processing activities, including the purpose of processing and retention periods, and keeps this up to date so that it reflects current processing activities.

16. Data Protection Officer

Thrive Tribe does not meet the ICO's criteria requiring the appointment of a formal Data Protection Officer. Data protection matters are managed by the Director.

17. Policy Review

This policy is reviewed by the Director at least annually, or more frequently where there is a significant change in circumstances.

To be disseminated to: Staff, volunteers, stakeholders, visitors		**Version no.** 003
Authorised by: Director	**Issue Date:** July 2026	**Review Due:** July 2027
Amendments: GoHighLevel included and old software deleted		