SCOPE

This document establishes the Galliford Try Employment Limited Data Protection Policy. References in this policy to the 'Company' are to Galliford Try Employment Limited. References in this policy to 'our people' are to employees of Galliford Try Employment Limited.

Galliford Try Employment Limited ('the Company') is fully committed to ensuring compliance with the requirements of the Data Protection Act 1998 (the 'Act'), and other privacy regulations. We regard the lawful and correct treatment of personal data as important to our successful operations and to maintain confidence within the Company and between us and those with whom we interact. We operate and maintain procedures to ensure that anyone who uses, holds, has access to or otherwise processes personal data in the course of their employment with the Company are fully aware of, and abide by their duties under this policy in respect of data protection.

Compliance with this policy is mandatory and any breach is taken seriously, and may result in disciplinary action being taken in accordance with the Galliford Try Employment Limited Disciplinary policy.

PURPOSE

The purpose of the policy is to protect the rights and privacy of individuals, and to ensure that data about them is not processed without their knowledge and is processed with their consent wherever possible.

The Galliford Try Employment Limited Data Protection Policy will be brought to the attention of all our people. The Policy does not form part of our people's contract of employment and may be amended by the Company from time to time. It will be reviewed annually.

DATA PROTECTION POLICY

1. Data Protection Definitions

1.1 "Data" is information which is stored electronically, on a computer, or in certain paper-based filing systems.

1.2 "Personal Data" means data relating to a living individual who can be identified from that data (or from that data and other information in, or likely to come into, possession of the Company). "Sensitive Personal Data" is a specific type of Personal Data which due to its nature is subject to a higher standard of protection.

1.3 "Processing" of personal data covers any activity that involves the use that data, including obtaining, recording or holding the data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing, destroying it or transferring to one or more third parties.

2. General Principles

Anyone in the Company who processes personal data is obliged to comply with the eight enforceable data protection principles. These provide that personal data must be:

- **Processed fairly and lawfully**. The Act is not intended to prevent data processing, but to ensure that it is done fairly and without adversely affecting an individual's rights.
- **Process for limited and specified purposes and in an appropriate way**. This means that Personal Data may only be processed for the specific purposes for which the data was first collected or for any other purposes permitted by the Act
- **Adequate, relevant and not excessive for those purposes**. Personal data should only be collected to the extent that it is required for a specific purpose: any data which is not necessary for that purpose should not be collected in the first place
- **Accurate and up to date.** Personal data must be accurate and kept up to date, with any inaccurate data being securely destroyed.
- **Not kept longer than is necessary for the purposes**. This means that data should be destroyed or erased from our systems when it is no longer required.
- **Processed in line with data subjects' rights**. An individual has certain rights under the Act, including requesting access to any data held about them by a data controller
- **Secure against unauthorized or unlawful processing and accidental loss, destruction and damage**. We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, personal data.
- **Not transferred to people or organisations situated in countries without adequate protection**. This requires us to take steps to ensure that where we transfer personal data to any third party we have checked that they have appropriate safeguards in place, particularly if they reside outside of the UK.

3. Data Security Breaches

Any breach of this policy, whether deliberate, or through negligence must be reported to the Data Protection Officer (see section 7 below). The Data Protection Officer will identify any on-going risks as a result of the breach and may notify the Information Commissioner's Office ("ICO"). Please note that failure to report any breach of this policy may lead to disciplinary action being taken under the Galliford Try Employment Limited Disciplinary policy.

4. Subject Access Requests

Under the Act, an individual can request access to personal data about them held by the Company by writing to us (including via electronic means such as e-mail or social media). This is known as a "Subject Access Request". The request must be accompanied by:

- sufficient detail to enable the data to be identified
- a fee of £10 paid in advance.

Subject Access Requests must be responded to within 40 days from receipt of the request and in accordance with Section 7 of the Act.

The Data Protection Officer will be responsible for ensuring the processing of Subject Access Requests is completed.

5. Third Party Processing

5.1 Where possible, we will use reasonable endeavours to inform any individual whose personal data is sent outside the company. Employee and other third party personal data may be used as follows:

- Information relating to their qualifications and career experience, normally in the form of a Curriculum Vitae (CV), may be used internally and included when appropriate in proposals sent to clients in the UK or overseas.
- Where applicable, personal information released to a new employer under the circumstances of a transfer under the Transfer of Undertakings Protection of Employment Act 1981 (TUPE), for the purposes of ensuring a smooth transfer to the new employer.
- Where applicable, personal information released to service providers which undertake tasks on our behalf e.g. payroll, Sharesave or flexible benefit providers

5.2 Personal data relating to individuals who are assigned (or who are being considered for an assignment) to work in other areas of the Galliford Try organization, may also be sent to senior management responsible for the project or office where they will be based. Such information will be held in conditions that have a similar level of security as in the sending organisation.

Only those third parties who have a strict requirement to receive personal data should be given access to it. If Personal data is transferred to, or accessed by a third party, appropriate contractual provisions will need to be included in an agreement between the Company and the third party, and appropriate technical and organizational measures should be put in place to protect the data.

6. Sensitive Personal Data

If any information that we hold about an individual is Sensitive Personal Data (for example, concerning their health, marital status, sexual orientation and religious beliefs), then you should use this information only for the purpose for which it was provided and do not store this information in the relevant databases, unless you have that person's consent to do so. For example, this information should not be transferred to a third party unless we have the individual's explicit consent to do so.

7. Data Protection Officer

We have appointed a Data Protection Officer who is responsible for the monitoring and implementation of this policy. The Data Protection Officer will act as the first point of contact for any Data Protection queries or matters.

8. Useful Contacts

HR Hub by telephone on 01455 231828 or by email to HR.Hub@gallifordtry.co.uk.
HR Contacts for advice and guidance.
The Data Protection Officer who is Mark Cotton, Chief Information Officer at mark.cotton@gallifordtry.co.uk