# Data Protection Policy – GDPR Compliant

Confidentiality and data protection are major issues within all workplaces, and this is reflected within the frameworks. There is legislation that is pertinent to confidentiality and data protection.

The major acts are:

- The Data Protection Act 1998
- GDPR
- The Access to Medical Reports Act 1998
- The Access to Health Records Act 1990
- The Freedom of Information Act 2000

The UK Data Protection Act 2018 (DPA 2018) and the European Union General Data Protection Regulation (GDPR) has clear guidelines concerning the storing and processing of PII (Personal identifiable information). "Personal identifiable information" means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This includes a wide range of personal identifiers including name; national insurance number; location data; telephone number; email address; job title; and online identifier.

The GDPR aims to prevent security breaches and the loss of personnel data by any organisation that holds or processes such data. The regulation change affects any organisation that processes personnel data. Doctore On Track Training Services Ltd are actively making changes to any relevant part of our business affected by the directive.

## 1. General Arrangements

When dealing with personal data, Doctore On Track Training Services Ltd representatives shall ensure that:

- **Data is processed fairly, lawfully and in a transparent manner** - personal information shall only be collected from individuals if representatives have been open and honest about why they want the personal information.
- **Data is processed for specified purposes only** - data shall only be collected for specific, explicit and legitimate purposes.
- **Data is relevant to what it is needed for** - data shall be monitored so that neither too much nor too little is kept; only data that is needed shall be kept.
- **Data is accurate and kept up to date and is not kept longer than it is needed** - personal data shall be accurate and, if it is not, it shall be corrected. Data no longer needed shall be deleted/shredded or securely disposed of.
- **Data is processed in accordance with the rights of individuals** - Individuals shall be informed, upon request, of all the personal data held about them.
- **Data is kept securely** - there shall be protection against unauthorised or unlawful processing of data and against accidental loss, destruction or damage.

We will process data about staff for legal, personnel, administrative and management purposes and

to enable us to meet our legal obligations as an employer, for example to pay you, monitor your performance and to confer benefits in connection with your employment. Transfers of personal data to countries located outside of Europe are restricted, so check with the Managing Director before taking mobile devices abroad with the intention of checking company emails or undertaking work, publishing personal data to the internet on the company's or another's website or sending information including personal data to a person or company outside of Europe.

We will only process "special category data" about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, biometric or genetic data held for purposes of identifying individuals, where a further condition is also met. We may process sensitive personal data relating to staff including, as appropriate:

- information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;
- the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation; and/or
- in order to comply with legal requirements and obligations to third parties.

We will keep the personal data we store about you accurate and up to date. Please notify us if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.

We will only process information about criminal proceedings or convictions as authorised by Data Protection Legislation.

We will not keep your personal data for longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required.

## 2. Storage

Data shall be securely kept at a Doctore On Track Training Services Ltd office and shall not be available for public access. All data stored on hardware shall be password protected and passwords shall be routinely changed. Once data is no longer needed, is out of date or has served its use or falls outside of any minimum retention time, it shall be shredded or securely deleted from the computer.

For absolute clarity, Network Rail requires Doctore On Track Training Services Ltd, as an NSAR assured training & assessment provider, to keep all training and assessment paper records for a period of 7 years following the training/assessment event and, to that end, secure archiving may be used. In addition, Doctore On Track Training Services Ltd cloud-based activities only use UK located servers.

All QCF evidence and records are confidential information and portfolios, assessor and internal verifier records are kept in a safe place to ensure that unauthorised people do not have access to them. Storage of evidence, confidentiality and data protection policies are discussed and documented by the candidate and assessor during completion of the pre-assessment checklist. Internal verifiers check to ensure these policies have been discussed and understood by checking for signatures and interviewing candidates. Where candidate portfolio's are used and kept at a workplace, they should ideally it should be in a locked cupboard.

## 3. Right to access

Doctore On Track Training Services Ltd is aware that individuals have the right to access any personal data that is held about them. Requests must be submitted in writing either in hard copy or via email. Doctore On Track Training Services Ltd is not able to disclose any personal information of any other individual other than themselves.

Individuals also have the right to have their data rectified if it is incorrect, the right to request erasure of the data, the right to request restriction of processing of the data and the right to object to data processing other than, **on all counts**, where that data and its use demonstrably relates to Sentinel notifiable rail training or assessments that have taken place and where that data is required to support compliance with the RTAS or Sentinel Scheme Rules or Network Rail or NSAR requirements.

## 4. Confidentiality

Doctore On Track Training Services Ltd representatives shall ensure the confidentiality of all complaints, appeals or other enquiries that are made to the company; they shall remain confidential unless the subject gives permission to disclose or where it would be otherwise unlawful not to disclose. When handling personal data, this shall also remain confidential.

These records may be used for reports both internally within Doctore On Track Training Services Ltd and to external bodies working with Doctore On Track Training Services Ltd in administration, including information required for financial administration a candidate, assessor or internal verifier has the right to ask to see details of any personal information Doctore On Track Training Services Ltd has stored about them. A request must be made in writing.

## 5. Confidential records used as evidence (SQA related activity only)

Candidates may quite appropriately cite service users' confidential records as evidence in their QCF qualification as long as the service user, or their advocate has given permission and informed consent for records to be used for this purpose. Confidential records should never be included in candidates' portfolios of evidence and should be examined in situ by the assessor. Assessors/candidates should describe and record what evidence such documents provide and where the evidence is located.

External verifiers may wish to discuss such evidence with the centre as part of the verification process but would not normally require sight of confidential service user's records.

However, should the EV have concerns about the quality of such evidence, they will, after discussion with their lead verifier, acquaint the centre management with their concerns, and seek consent to access such records from the organisation which has responsibility for the safe keeping of the particular service user's confidential records in question.

## 6. Data Breach

GDPR defines a personal data breach as "a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor

- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Any breach in the security of the assessment materials published on the SQA secure site / NSAR Tool kit site must be reported immediately to SQA or NSAR respectively.

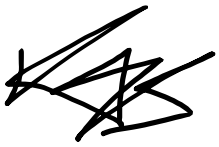
Any transport of material between assessment sites shall be secure and agreed between candidate and assessor prior to transportation to minimise risk of a breach.

This policy, and its supporting objectives and targets will be communicated to all personnel, clients, associates, suppliers and sub-contractors and also to the general public where appropriate to make sure they are fully aware and understand the content of this policy and comply with it. It is the responsibility of everyone to highlight any deficiencies found within this policy. Any wilful failure to comply with this policy or any individual involvement in a data breach shall be viewed as Gross Misconduct.

Doctore On Track Training Services Ltd is a member of the Information Commissioners Office and our membership number is ZA671716.

It is the responsibility of the Managing Director to ensure that this policy is kept up to date and regularly reviewed for compliance, suitability and practicality. This policy shall be reviewed on an annual basis.

Signed



Managing Director
31st December 2024