



Green State Innovation and Training Ltd

Data Protection Policy



1. Introduction

Green State Innovation and Training Ltd ("the Company") is committed to safeguarding the privacy and security of personal data. As a small training provider working closely with awarding bodies, we recognize the importance of complying with data protection laws, including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy outlines our approach to data protection and the procedures we have in place to ensure that personal data is handled responsibly and securely.

2. Scope

This policy applies to all employees, contractors, volunteers, and partners who process personal data on behalf of Green State Innovation and Training Ltd. It covers all personal data, regardless of its format (electronic, paper, etc.), that is collected, stored, processed, or shared by the Company.

3. Data Protection Principles

We adhere to the following data protection principles:

1. Lawfulness, Fairness, and Transparency

Personal data shall be processed lawfully, fairly, and in a transparent manner.

2. Purpose Limitation

Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Data Minimization

Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

4. Accuracy

Personal data shall be accurate and, where necessary, kept up to date.



5. Storage Limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. Integrity and Confidentiality

Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.

4. Legal Basis for Processing

Green State Innovation and Training Ltd will only process personal data where there is a legal basis to do so. The legal bases include:

- **Consent:** The data subject has given clear consent for their personal data to be processed for a specific purpose.
- **Contract:** The processing is necessary for a contract with the data subject, or because they have asked us to take specific steps before entering into a contract.
- **Legal Obligation:** The processing is necessary to comply with the law.
- **Legitimate Interests:** The processing is necessary for our legitimate interests, unless these are overridden by the data subject's rights and interests.

5. Data Subject Rights

Data subjects have the following rights regarding their personal data:

- **Right to be Informed:** The right to be informed about the collection and use of their personal data.
- **Right of Access:** The right to access their personal data and supplementary information.
- **Right to Rectification:** The right to have inaccurate personal data rectified or completed if it is incomplete.



- Right to Erasure: The right to have personal data erased, also known as the 'right to be forgotten'.
- Right to Restrict Processing: The right to request the restriction or suppression of their personal data.
- Right to Data Portability: The right to obtain and reuse their personal data for their own purposes across different services.
- Right to Object: The right to object to the processing of their personal data in certain circumstances.
- Rights Related to Automated Decision-Making: The right not to be subject to a decision based solely on automated processing, including profiling.

6. Data Collection and Processing

We collect and process personal data only for legitimate business purposes, such as:

- Managing learner records.
- Communicating with awarding bodies.
- Handling administrative tasks related to training and certification.
- Complying with legal obligations and regulatory requirements.

7. Data Sharing

We may share personal data with third parties, such as awarding bodies, for legitimate purposes. All data sharing is conducted in a manner that ensures the security and confidentiality of the data. Third parties are required to adhere to our data protection standards.

8. Data Security

We implement appropriate technical and organisational measures to protect personal data against unauthorised access, loss, destruction, or damage. This includes:



- Secure storage of electronic data using encryption and access controls.
- Secure storage of paper records in locked cabinets.
- Regular data protection training for staff.
- Procedures for securely disposing of personal data that is no longer needed.

9. Data Retention

Personal data will only be retained for as long as necessary to fulfill the purposes for which it was collected or as required by law. Once data is no longer needed, it will be securely deleted or destroyed.

10. Data Breach Response

In the event of a data breach, Green State Innovation and Training Ltd will act promptly to mitigate the impact, investigate the breach, and notify the relevant authorities and affected data subjects, as required by law.

11. Responsibilities

- **Data Protection Officer (DPO):** The DPO is responsible for overseeing data protection compliance, providing guidance to the organisation, and serving as the contact point for data protection issues.
- **Employees and Contractors:** All employees and contractors are responsible for ensuring compliance with this policy and for reporting any potential data protection risks to the DPO.

12. Training and Awareness

All employees, contractors, and volunteers will receive regular training on data protection principles and practices. New staff members will receive data protection training as part of their induction process.

13. Policy Review



This policy will be reviewed annually or whenever there are significant changes in data protection laws, business practices, or data processing activities.