Several Seats CIC

Data Protection and Data Secruity Policy

Our Policy

Several Seats Policy

DATA PROTECTION AND DATA SECURITY POLICY

Statement and purpose of the policy

A. Several Seats C.I.C (the Employer) is dedicated to ensuring that all personal data handled by the organization is processed in line with legal standards for data protection and security.

B. For the purposes of data protection laws, the Employer is considered the data controller, meaning it determines the purposes and means of processing personal data in relation to your employment.

C. The purpose of this policy is to support the Employer's compliance with data protection and security obligations by:

1. **Informing staff about the types of personal information collected, and how we handle it.**
2. **Clarifying the legal rules and conditions for collecting, processing, storing, and sharing personal data.**
3. **Defining staff responsibilities in relation to data protection and security.**

D. This policy is a statement of guidelines only and does not form part of your employment contract. The Employer reserves the right to amend this policy as needed.

E. Definitions:

1. **Criminal records data: Information on convictions, offences, and related allegations.**
2. **Data protection laws: The UK General Data Protection Regulation (UK GDPR) and all applicable data privacy laws.**
3. **Data subject: The individual whose personal data is processed.**
4. **Personal data: Information relating to an identifiable person.**
5. **Processing: Any operation on data, including collection, storage, amendment, and deletion.**
6. **Special categories of personal data: Data about an individual's racial or ethnic origin, political beliefs, health, or sexual orientation.**

Data Protection Principles

All staff must comply with the following data protection principles:

1. **Lawfulness, fairness, and transparency: Processing must have a lawful basis.**
2. **Purpose limitation: Data should only be used for specified, legitimate purposes.**
3. **Data minimization: Only data necessary for the purpose should be collected.**
4. **Accuracy: Data must be accurate and kept up to date.**
5. **Storage limitation: Personal data must only be retained for as long as necessary.**
6. **Integrity and confidentiality: Data must be processed securely to protect against unauthorized access, loss, or destruction.**

Responsibilities for Data Protection and Security

Maintaining compliance is the shared responsibility of both the Employer and its staff. All staff, regardless of their position, are responsible for following this policy.

1. **Staff responsibilities: Ensure the security of personal data and report any suspected breaches to the Data Protection Officer.**
2. **Management responsibilities: Monitor staff compliance and report policy violations.**
3. **Breach of policy: Violations may result in disciplinary action, including dismissal in serious cases.**

Personal Data and Sensitive Information

We process various categories of personal data, including but not limited to:

- **Home address, contact details, and next of kin information.**
- **Employment records, such as CVs, references, and performance reviews.**
- **Sensitive information, such as health or criminal records, where legally allowed and necessary.**

Before processing sensitive personal data, an assessment must be conducted to ensure compliance with legal criteria, and individuals will be informed of how and why their sensitive data is processed.

How We Use Your Data

The Employer processes personal data for several purposes, including:

- **Business operations and administration.**
- **Managing employment contracts, pay, and performance reviews.**
- **Monitoring IT usage and ensuring compliance with disciplinary procedures.**

We ensure that all processing is relevant, accurate, and complies with our privacy notice.

Storage, Retention, and Security of Data

Personal data is stored securely, in line with our Information Security Policy. It is retained only for the necessary period, in accordance with our data retention policy.

Security procedures include:

- **Using strong passwords and locking computers when unattended.**
- **Encrypting or password-protecting data stored on portable devices.**
- **Keeping physical documents in locked storage and securely disposing of them when no longer needed.**

Rights of Individuals

Under data protection laws, individuals have rights regarding their personal data. These include:

- **Access: Request access to the personal data we hold about you.**
- **Correction: Request corrections to inaccurate or outdated data.**
- **Erasure: Ask for personal data to be erased if it is no longer necessary.**
- **Restriction: Limit how your data is processed.**
- **Objection: Object to data processing based on legitimate interests.**

To exercise these rights, contact us at team@severalseats.org. We may request proof of identity and will respond within legal timeframes.

Data Breaches

In the event of a data breach that poses a risk to individual rights, the Employer will report it to the Information Commissioner within 72 hours and notify affected individuals where necessary.

International Transfers of Data

If personal data is transferred outside the UK or the European Economic Area (EEA), we ensure that adequate protections are in place in accordance with data protection laws.

Training

All staff will receive training on data protection and security responsibilities as part of their induction and at regular intervals. Specific staff, such as managers and those with data access, will receive additional training.

Review

This policy will be regularly reviewed to ensure it remains compliant with current legislation and industry standards. The next scheduled review will take place during the Board of Directors' meeting on 29th March 2025.