FIRST PERSON PROJECT C.I.C.

Policy

Policy Number:	008
Policy Title:	Data Protection and Best Practice
Scope of this Document:	All Staff (including employees and volunteers) All contractors
Recommending Committee:	Quality and Safety Committee
Approving Committee:	First Person Project Board of Directors
Date Ratified:	17/10/23
Review Period:	3 Years
Version number:	1.0
Lead Executive Director:	Matty Caine
Author(s):	Matty Caine

FIRST PERSON PROJECT C.I.C.

Progressing Together

Contact:	Johnathan Ormond-Prout: johnathan@firstpersonprojectcic.co.uk Matty Caine: matty@firstpersonprojectcic.co.uk
Published by:	First Person Project CIC https://www.firstpersonprojectcic.co.uk/

Version Control:			
Version	**Reason for Change**	**Change Author**	**Change Date**
1	Original Policy	MC	17/10/23

First Person Project Data Protection and Best Practice Policy

Effective Date: 17th Oct 2023

1. Introduction

This policy sets forth the commitment of First Person Project CIC to protect the data of our clients, staff, volunteers, and other stakeholders. Compliance with the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 is a priority, reflecting our dedication to privacy and data protection.

2. Scope

This policy applies to all staff, volunteers, contractors, and any other individuals working on behalf of First Person Project CIC.

3. Definitions

Personal data: Information relating to an identifiable person, including names, addresses, email addresses, health information, etc.
Sensitive data: Special categories of personal data, such as health information, racial or ethnic origin, religious beliefs, etc.
Processing: Operations performed on personal data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, alignment, combination, restriction, erasure, or destruction.

4. Data Protection Principles

We are committed to processing data in accordance with the following principles:

- Lawfulness, fairness, and transparency: Processing in a lawful, fair, and transparent manner.
- Purpose limitation: Collected for specified, explicit, and legitimate purposes.
- Data minimisation: Adequate, relevant, and limited to what is necessary.

- Accuracy: Accurate and, where necessary, kept up to date.
- Storage limitation: Kept in a form that permits identification for no longer than necessary.
- Integrity and confidentiality: Processed securely to ensure appropriate confidentiality, integrity, availability, and resilience.

5. Staff and Volunteer Responsibilities

- Awareness: Be aware of this policy and understand individual responsibilities.
- Access control: Only access personal data when necessary and if authorised.
- Data accuracy: Ensure accuracy of data and report any errors or discrepancies.
- Confidentiality: Uphold confidentiality and not disclose personal data improperly.
- Training: Complete all required data protection training and stay updated on new practices.
- Breach reporting: Immediately report any suspected data breaches to the DPO.

6. Data Subject Rights

We respect the rights of individuals, including:

- Access: Right to request access to personal data held about them.
- Rectification: Request correction of incorrect personal data.
- Erasure: Request deletion of personal data in certain circumstances.
- Restriction of processing: Restrict processing of personal data.
- Data portability: Obtain and reuse personal data.
- Object: Object to the processing of personal data.

7. Data Protection Officer (DPO)

Our DPO oversees data protection strategies and ensures compliance.

DPO Contact Details: Johnathan Ormond-Prout, johnathan@firstpersonprojectcic.co.uk

8. Data Security

Physical and digital security measures: Implemented to protect data integrity and prevent unauthorized access.
Regular reviews: Regularly review and update security practices.

9. Breach Response

Identification and assessment: Quickly identify and assess any potential data breaches.
Notification: Notify the relevant authorities and affected individuals where necessary.

10. Training and Awareness

Regular training sessions: We provide regular data protection training for all staff and volunteers, upon induction and yearly thereafter.
Updates on legislation: Keep updated on changes in data protection laws and best practices.

11. Policy Review and Update

This policy will be reviewed in 3 years and updated as necessary to ensure ongoing compliance.

12. Consequences of Non-Compliance

Non-compliance with this Data Protection and Best Practice Policy by staff or volunteers can lead to serious consequences for the individual(s) involved and the organisation as a whole.

A. For the Individual:

Disciplinary Action: Non-compliance will result in disciplinary action, which may include verbal or written warnings, suspension, or termination of employment or volunteering duties.
Legal Action: In cases of serious breaches, legal consequences including fines or legal proceedings.
Professional Repercussions: Impact on the individual's professional reputation and future employment opportunities.

B. For the Organisation:

Financial Penalties: Substantial fines for non-compliance.

Reputational Damage: Loss of trust from clients, donors, and the community.

Operational Disruptions: Impact on service delivery and organisational efficiency.

Legal and Regulatory Scrutiny: Increased scrutiny and potential loss of licenses or certifications.

C. Reporting and Addressing Non-Compliance:

Immediate Reporting: Any suspected non-compliance or data breach must be reported immediately to the DPO.

Investigation: Thorough investigation of all reports.

Support and Training: Continuous support and training for staff and volunteers.