

Data Protection and GDPR Compliance Policy

1.0 Introduction and Purpose

Impact-Inspire is committed to upholding the highest standards of data protection and privacy. We understand that the lawful, fair, and transparent handling of personal data is fundamental to maintaining the trust of our employees, clients, partners, and the public. Our reputation and the integrity of our services depend on our ability to protect personal information.

The purpose of this policy is to establish a comprehensive framework that ensures all personal data is processed in full compliance with the UK General Data Protection Regulation (UK GDPR) / Data Protection Act 2018, and all other relevant data protection legislation. It outlines our approach to data handling, defines responsibilities, and provides clear guidance to all personnel to ensure we meet our legal and ethical obligations.

2.0 Scope

This policy applies to all personal data processed by Impact-Inspire, regardless of the format (e.g., electronic, paper) or where it is stored. It covers all company personnel, including directors, employees, contractors, volunteers, and any other individuals or entities processing data on behalf of Impact-Inspire.

Adherence to this policy is mandatory.

3.0 Guiding Data Protection Principles

Impact-Inspire adheres to the data protection principles enshrined in the UK GDPR. We are committed to ensuring that all personal data is:

1. **Processed lawfully, fairly, and in a transparent manner** (Lawfulness, Fairness, and Transparency).
2. **Collected for specified, explicit, and legitimate purposes** and not processed in a way that is incompatible with those purposes (Purpose Limitation).
3. **Adequate, relevant, and limited to what is necessary** for the purposes for which it is processed (Data Minimisation).
4. **Accurate and, where necessary, kept up to date**, with every reasonable step taken to erase or rectify inaccurate data without delay (Accuracy).
5. **Kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which it is processed (Storage Limitation).
6. **Processed in a manner that ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage (Integrity and Confidentiality).
7. **Accountability**: Impact-Inspire is responsible for, and must be able to demonstrate, compliance with these principles (Accountability).

4.0 Roles and Responsibilities

4.1 Data Protection Lead

Impact-Inspire has appointed a Data Protection Lead who is responsible for:

- Informing and advising the organisation and its personnel about their obligations under data protection law.

- Monitoring compliance with this policy and relevant legislation.
- Acting as the primary point of contact for data subjects and the Information Commissioner's Office (ICO).
- Providing guidance on Data Protection Impact Assessments (DPIAs).

4.2 Senior Management

Senior management is responsible for championing a culture of data protection, ensuring adequate resources are allocated for compliance, and integrating data protection into all organisational processes.

4.3 All Personnel

All personnel who handle personal data have a duty to:

- Process data only for the legitimate purposes for which it was collected.
- Handle data securely and in line with this policy and associated procedures.
- Complete mandatory data protection training.
- Report any data breaches or security concerns immediately.

5.0 Lawful Processing of Data

All processing of personal data will be based on a valid lawful basis as defined under the UK GDPR. We will identify and document the appropriate basis for each processing activity. Where we process special category (sensitive) data, we will identify both a lawful basis under Article 6 and a separate condition for processing under Article 9 of the UK GDPR.

A Data Protection Impact Assessment (DPIA) will be conducted for any new or significantly changed processing activity that is likely to result in a high risk to the rights and freedoms of individuals.

6.0 Data Subject Rights

Impact-Inspire fully respects and will facilitate the rights of data subjects. Any individual whose data we process has the right to:

- **Be informed** about how their data is being used.
- **Access** their personal data.
- **Rectify** inaccurate personal data.
- **Erase** personal data in certain circumstances (the 'right to be forgotten').
- **Restrict** the processing of their personal data.
- **Data portability** of their personal data.
- **Object** to the processing of their personal data.
- Rights related to **automated decision-making and profiling**.

Requests to exercise these rights should be directed to the Data Protection Lead and will be handled promptly and in accordance with legal timeframes.

7.0 Data Security Measures

We are committed to ensuring the security of all personal data we process. We have implemented appropriate technical and organisational measures to protect data against unauthorised access, accidental loss, destruction, or damage. These measures include:

- **Access Control:** Restricting access to personal data to authorised personnel on a need-to-know basis.
- **Encryption:** Using encryption for data in transit and at rest where appropriate.
- **Physical Security:** Securing physical records and IT equipment in locked cabinets and offices.
- **Secure Data Transfer:** Utilising secure methods for transferring data internally and externally.

- **Supplier Due Diligence:** Ensuring that any third-party processors provide sufficient guarantees of their data protection measures.

8.0 Data Breach Response

Impact-Inspire has a clear procedure for responding to any personal data breach. In the event of a suspected breach:

1. All personnel must report the incident immediately to their line manager and the Data Protection Lead.
2. The Data Protection Lead will lead an investigation to assess the nature and severity of the breach.
3. If the breach is likely to result in a risk to the rights and freedoms of individuals, the ICO will be notified within 72 hours of us becoming aware of it.
4. If the breach is likely to result in a high risk, the affected individuals will also be informed without undue delay.
5. All breaches, regardless of their severity, will be documented in an internal breach register.

9.0 Training and Awareness

Data protection is a shared responsibility. All personnel will receive mandatory data protection training upon induction and will be provided with regular refresher training. We are committed to fostering a culture of continuous awareness, ensuring that all team members understand their roles and responsibilities in protecting personal data.

10.0 Policy Review and Continuous Improvement

This Data Protection and GDPR Compliance Policy will be reviewed at least annually by the Data Protection Lead and senior management. It will also be updated in response to any changes in legislation, regulatory guidance,

or our business practices to ensure its ongoing effectiveness and our continued compliance.

Version Number	Author	Purpose / Change	Date
1.0	Reece Casey	Policy Created	30 th November 2025