##

Data Protection Policy

#

|  |
| --- |
| Purpose of this document |
| This document sets out how Inspire North complies with the Data Protection Act.  |
| **Date:** | July 2020 | **Review Due:** | July 2023 |
| **Version No.:** | 1.2 | **Review Frequency:**  | 3-yearly |
| Classification: This document is for Inspire North internal use only |

****

**1.0 Introduction**

##  **What is the purpose of this policy?**

##  Inspire North has both a moral and legal obligation to safeguard all data in its possession. This includes information on any individuals including employees, clients, charity trustees, directors, contacts, suppliers and supporters.

##  Inspire North is committed to complying with all relevant privacy and data protection laws including:

1.3.1 The Data Protection Act 2018 (DPA) and the General Data Protection Regulation 2016 (GDPR) and any related legislation which applies in the UK.

1.3.2 The Privacy and Electronic Communications Regulations and any successor or related legislation, including the E-Privacy Regulation; and

### All other applicable laws and regulations relating to the processing of personal data and privacy and, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office ("ICO") or any other supervisory authority.

1.4 This policy sets out what we do to protect individuals' personal data.

1.5 Anyone who handles personal data in any way on behalf of Inspire North must ensure that they comply with this policy.

1.6 Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

1.7 This policy may be amended from time to time to reflect any changes in legislation, regulatory guidance or internal policy decisions.

1.8 All employees should ensure they familiarise themselves with this Policy.

1.9 Inspire North does not have a specific data protection officer as it falls outside the requirements to do so, however the responsibility for Data Protection at Inspire North resides with the Director of Finance and Corporate Services.

**2.0 About this Policy**

2.1 The types of personal data that we may process include details of:

* Clients / tenants;
* Employees;
* Trustees;
* Volunteers
* Contractors
* Contacts;
* Supporters; and
* Event attendees.

2.2 This policy must be applied in conjunction with all other relevant policies and manuals as outlined in the Information Governance Framework, available on the Intranet.

## **2.3 Definitions and common terms**

The following terms will be used in this Policy:

|  |  |
| --- | --- |
| **Data Subjects** | All living individuals about whom we hold personal data, for instance an employee or a client.All data subjects have legal rights in relation to their personal data. |
| **Personal Data**  | Data that relates to a living individual, who can be identified from that data, or from a combination of that data and other information held by, or likely to come into the possession of, the Data Controller or Data Processor. Examples include HR records for office or field staff, medical records, supporter information, membership records, contact databases. |
| **Data Controller** | The person or organisation who collects, processes and manages personal data, and has a legal basis for doing so. |
| **Data Processors** | Any third party who processes personal data on behalf of Inspire North. |
| **EEA** | Includes all countries in the European Union as well as Norway, Iceland and Liechtenstein. |
| **ICO**  | Means the Information Commissioner's Office (the authority which oversees and enforces data protection regulation in the UK). |
| **Processing**  | Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as:* collection,
* recording,
* organisation,
* structuring,
* storage,
* adaptation or alteration,
* retrieval,
* consultation,
* use,
* disclosure by transmission,
* dissemination or otherwise making available,
* alignment or combination,
* restriction,
* erasure or destruction.
 |
| **Sensitive Personal Data / Special Category Data**  | This is personal data revealing: * racial or ethnic origin;
* political opinions;
* religious or philosophical beliefs;
* trade union membership;
* genetic data;
* biometric data for the purpose of uniquely identifying a natural person;
* data concerning health; or
* data concerning a natural person's sex life or sexual orientation.
 |

## **3.0 Data Protection Principles**

3.1 Anyone processing personal data must comply with the six data protection principles as set out in the legislation.

3.2 We are required to comply with these principles (summarised in Appendix 1), and show that we comply, in respect of any personal data that we deal with as a data controller.

3.3 Personal data should be:

1. Processed fairly, lawfully and transparently;
2. Collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary for the purpose for which it is held;
4. Accurate and, where necessary, kept up to date;
5. Not kept longer than necessary; and
6. Processed in a manner that ensures appropriate security of the personal data.

## **4.0** **Transferring Data Outside the UK and EEA**

4.1 Inspire North does not usually transfer data outside the UK. Should in exceptional circumstances Inspire North be required to transfer data outside the UK or the EEA it will ensure that the transfer is undertaken in line with the requirements of the DPA and GDPR and take steps to ensure that the data is properly protected.

**5.0** **Processing Special category (Sensitive personal) data**

5.1 Inspire North collects information about individuals that is defined by the GDPR as **special categories of personal data,** and special rules will apply to the processing of this data (these categories are set out in Section 2.1).

5.2 Purely financial information is not technically defined as sensitive personal data by the GDPR. But should be treated in a similar way as it can have a significant impact on an individual if it is misused.

5.3 When processing special category data, we will always ensure that the appropriate conditions for processing are applied.

## **5.4 Processing Children’s Data (Under the age of 13)**

5.5 There are certain requirements under the GDPR that apply where organisations offer services to children. Whilst Inspire North does hold personal data about Children as part of a family group, it does not offer services directly to children under the age of 13.

## **6.0 Notification**

We recognise that whilst there is no obligation for us to make an annual notification to the ICO under the Data Protection Act or GDPR, we will consult with the ICO where necessary when we are carrying out "high risk" processing.

## **7.0 Personal Data Breaches**

7.1 We will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary, within 72 hours.

7.2 We will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individuals.

7.3 The role of the SIRO during a data breach is to support and advise the Leadership team during incident management on:

* relevant data protection legislation;
* what our requirements are;
* potential impacts to privacy; and
* clear guidance on whether a breach should be reported to the Regulator (ICO).

7.4 If, after taking everything into account, the Leadership team decide that a breach is reportable then the SIRO will liaise with the ICO.

7.5 Examples of a reportable data breach could potentially include:

* access to personal data by an unauthorised 3rd party;
* deliberate or accidental action (or inaction);
* sending personal data to an incorrect recipient;
* computing devices containing personal data being lost or stolen;
* alteration of personal data without permission; and
* loss of availability of personal data.

7.6 For further information please refer to the Inspire North Data Breach Incident Reporting and Management Process.

# 8.0 Record Keeping

8.1 A record of each business area’s data processing activities must be documented on an Information Asset Register (IAR). Inspire North have combined their IAR with the RoPA (Record of Processing Activity.

8.3 An IAR demonstrate that we are complying with relevant data protection legislation and include the purpose of processing, descriptions of categories of data subjects and categories of personal data, details of transfers to third countries and retention periods of personal data.

#

## **9.0 Data Protection by Design / Data Protection Impact Assessments**

9.1 We will implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities.

9.2 We will work to the current ICO guidance on privacy by design.

9.3 Carrying out Data Protection Impact Assessments (DPIAs) is an integral part of Inspire North’s privacy by design approach in achieving compliance with the relevant data protection legislation.

9.4 A DPIA will be carried out where any process, programme or project brief is being created e.g. change processes, service development, project and programme processes.

9.5 DPIAs must be conducted for changes to existing processes even if a DPIA has been carried out before.

9.6 For more information please see Inspire North’s Data Protection Impact Assessment (DPIA) procedure.

### **10.0 Contracts**

10.1 Where we engage in services with third party processors, we must follow the appropriate policies and procedures such as relevant procurement policies.

10.2 Where a third party is processing personal data on our behalf, we must ensure that adequate contracts are in place to protect Inspire North and the Data Subjects being processed.

10.3 Our contracts must include the following compulsory details:

* the subject matter and duration of the processing;
* the nature and purpose of the processing;
* the type of personal data and categories of data subject; and
* the obligations and rights of the controller.

10.4 We aim to comply with all good practice guidance for contracts and compulsory terms for third party processors to comply with the Data Processing Act are set out in appendix 2.

#

## **11.0 Responsibilities**

11.1 Inspire North Trustees and Senior Leadership Team are responsible for ensuring compliance with relevant data protection legislation. As an organisation we must:

* implement appropriate technical and organisational measures that ensure and demonstrate our compliance. This will include internal data protection policies, employee training, internal audits of processing activities, and reviews of internal HR policies;
* maintain relevant documentation on processing activities;
* implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
	+ data minimisation;
	+ pseudonymisation;
	+ transparency;
	+ allowing individuals to monitor processing; and
	+ creating and improving security features on an ongoing basis.
* use Data Protection Impact Assessments where appropriate.

11.2 We can also adhere to approved codes of conduct and/or certification schemes as approved by the ICO.

11.3 The **Senior Leadership Team**:

* are responsible for data risks for their area and are ultimately responsible for the data processed within it
* must ensure that all employees that they are responsible for are fully aware of relevant data policies and have been appropriately trained;
* ensure that their teams handle data appropriately and in line with relevant data legislation, this policy and all other relevant Inspire North policies;
* ensure that the right culture, tone and behaviours are embedded into the way that they work in order to protect Inspire North and the individuals that we process data for.

11.4 The **SIRO** has responsibility for data protection and as such is responsible for:

* Informing and advising Inspire North and its employees about their obligations to comply with relevant data protection legislation;
* Monitoring compliance with relevant data protection legislation including managing internal data protection activities, advising the business on DPIA’s where there are high risks, training of employees and carrying out internal reviews.

**Appendix 1**

**The 6 Data Protection Principles**

## **Processing Data Fairly and Lawfully**

The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about.

Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons, such as where it is necessary for the performance of a contract.

Certain information must be given to Data Subjects at the time of collecting the information or as soon as possible after having received the data.

This fair processing information can be provided in a number of places including on web pages, in mailings or on application forms. We must ensure that the fair processing information is concise, transparent, intelligible and easily accessible.

The table below outlines what information must be provided.

| **Information to be supplied** | **Data obtained directly from the data subject** | **Data not obtained directly from the data subject** |
| --- | --- | --- |
| The identity and contact details of the controller e.g. Inspire North and the SIRO  | ✓ | ✓ |
| Purpose and lawful basis of the processing | ✓ | ✓ |
| The legitimate interests of the controller | ✓ | ✓ |
| Categories of personal data |  | ✓ |
| Any recipient or categories of recipients of personal data | ✓ | ✓ |
| Details of where data is transferred to a third country | ✓ | ✓ |
| Retention period or criteria used to determine the retention period | ✓ | ✓ |
| The existence of each of the data subject’s rights  | ✓ | ✓ |
| The right to withdraw consent at any time, where relevant | ✓ | ✓ |
| The right to lodge a complaint with the ICO | ✓ | ✓ |
| The source the personal data originates from and whether it came from publicly accessible sources |  | ✓ |
| Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data | ✓ |  |
| The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences  | ✓ | ✓ |

## **Processing data for the original purpose**

The second data protection principle requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when we first obtained their information.

This means that we should not collect personal data for one purpose and then use it for another.

If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand and the legal basis for processing under the new purpose e.g. consent, legitimate interest.

## **Personal data should be adequate and accurate**

The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant.

Data should be limited to what is necessary in relation to the purposes for which it is processed.

Inaccurate or out-of-date data should be destroyed securely, and we must take every reasonable step to ensure that personal data which is inaccurate is corrected.

## **Not retaining data longer than necessary**

The fifth data protection principle requires that we should not keep personal data for longer than we need to for the purpose it was collected for.

This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer needed.

For guidance on how long particular types of personal data that we collect should be kept before being destroyed or erased, please see the Data Retention and Destruction Schedule Procedure.

## **Rights of Individuals under the GDPR**

The GDPR gives people rights in relation to how organisations process their personal data.

Everyone who holds personal data on behalf of Inspire North needs to be aware of these rights. They include the right:

1. to request a copy of any personal data that we hold about them (as data controller), as well as a description of the type of information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights);
2. to be told, where any information is not collected from the person directly, any available information as to the source of the information;
3. to be told of the existence of automated decision-making;
4. to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests;
5. to have all personal data erased (the right to be forgotten) unless certain limited conditions apply;
6. to restrict processing where the individual has objected to the processing;
7. to have inaccurate data amended or destroyed; and
8. to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

## **Data Security**

The sixth data protection principle requires that we keep secure any personal data that we hold.

We are required to put in place procedures to keep the personal data that we process and hold secure, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

When we are dealing with sensitive personal data, more rigorous security measures are likely to be needed.

When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

You should refer to the relevant Information and IT policies and procedures for guidance. If further support or guidance is needed, you should consult with the **SIRO.**

**Appendix 2**

**Compulsory terms for contracts with third party processors to comply with the Data Processing Act**

* the processor must only act on the written instructions of the controller (unless required by law to act without such instructions);
* the processor must ensure that people processing the data are subject to a duty of confidence;
* the processor must take appropriate measures to ensure the security of processing;
* the processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
* the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
* the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
* the processor must delete or return all personal data to the controller as requested at the end of the contract; and
* the processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the UK.