inspire community trust

General Data Protection Regulation (GDPR)

Statement of Policy

1. INTRODUCTION

The General Data Protection Regulation (GDPR), Data Protection Bill, requires employers to comply with the data protection principles, demonstrate their compliance and implement appropriate technical and organisational measures to ensure and demonstrate that they process data in accordance with the GDPR ensuring a level of security appropriate to the risk involved in processing.

2. POLICY STATEMENT

This policy is designed to ensure that Inspire complies with its legal responsibilities in relation to data. Inspire is committed to being transparent about how it collects and uses the personal data of its workforce and service users, and to meeting its data protection obligations. This policy sets out the Inspire's commitment to data protection, and individual rights and obligations in relation to personal data. All staff are expected to comply with the requirements of this policy.

This policy will be reviewed annually, or more frequently if required by regulation, legislation or good practice.

3. DEFINITION

The GDPR not only requires employers to comply with the data protection principles but to demonstrate that they comply. This is known as the principle of accountability. Employers are also required to implement appropriate technical and organisational measures (including implementing appropriate data protection policies and providing employee training) to ensure and demonstrate that they carry out processing in accordance with the requirements of the GDPR.

4. PURPOSE

This policy applies to the personal data processed for business purposes including, but not limited to, personal data of service users, relatives, job applicants, employees, workers, contractors, volunteers, work placements, apprentices and former employees.

Inspire has appointed the Chief Executive as its Data Protection Officer. His/her role is to inform and advise Inspire on its data protection obligations.. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.

5. CONTEXT

The General Data Protection Regulation (GDPR) (2016/679 EU), Data Protection Bill requires organisations to demonstrate that they carry out processing in accordance with the requirements of the GDPR.

6. IMPLEMENTATION

6.1	**Definitions**
6.2	**General Outline**
6.3	**Data Protection Principles**
6.4	**Written Records of Processing Activities**
6.5	**Individual Rights**
6.6	**Data Security**
6.7	**Impact Assessments**
6.8	**Data Breaches**
6.9	**International Transfers**
6.10	**Individual Responsibilities**
6.11	**Training and Instruction**

6.1 Definitions

“Data Controller” is Inspire Community Trust, 20 Whitehall Lane, Slade Green, Dartford, DA8 2DH

“Data Protection Officer” is the Chief Executive.
"Personal data" is any information that relates to an individual who is alive and can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

6.2 General outline

Organisations are required to appoint a Data Protection Officer under the GDPR if they are a public authority, their core activities include the regular and systemic monitoring of data subjects on a large scale, or their core activities consist of processing special categories of personal data or data relating to criminal convictions and offences on a large scale.

The GDPR and the Data Protection Bill place restrictions on the processing of special categories of personal data and data on criminal convictions and offences. Under the GDPR, special categories of personal data are defined as information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data. Data on criminal convictions and offences includes information relating to criminal allegations and proceedings. These types of data were previously known as "*sensitive personal data*" under the Data Protection Act 1998.

Employers are likely to rely on a condition in sch.1 to the Bill to process special categories of personal data or data relating to criminal convictions and offences, specifically that the data is processed because it is necessary to perform or exercise obligations or rights under employment law. Where this is the case, the Bill requires that the organisation's data register include information on additional safeguards, specifically:

- the condition relied on in sch.1 to the Bill to process the data;
- how the processing satisfies the requirement of lawful processing under the GDPR; and,
- whether or not the data is retained and erased in accordance with a policy as required under the Bill and, if it is not, the reasons why.

6.3 Data protection principles

Inspire processes personal data in accordance with the following data protection principles:

- personal data is processed lawfully, fairly and in a transparent manner.
- personal data is collected only for specified, explicit and legitimate purposes.
- personal data is processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Inspire keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- personal data is kept only for the period necessary for processing.
- appropriate security measures are adopted to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.
- Inspire tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Where Inspire processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

Inspire will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

Personal data gathered during the course of Inspire's business is held in the relevant files (e.g. care plans, personnel files, payroll files), in hard copy or electronic format, or both. The periods for which the Inspire holds personal data are contained in its privacy notices to individuals and registers.

6.4 Written records of processing activities

Where there is a specific obligation to maintain written records of processing activities. The record of processing activities must include:

- the name and contact details of the organisation, any joint controller and the data protection officer (if applicable);
- the purposes of the processing;
- a description of the categories of data subjects;
- a description of the categories of personal data;
- a description of the categories of recipients to whom data has been or will be disclosed;
- where applicable, information about transfers of data to countries outside the EEA or to any international organisation (which in both cases must be named) and, in some cases, details of the basis on which such transfers are made;
- the anticipated time limits for erasing different categories of data; and,
- a general description of the technical and organisational security measures adopted.

Inspire keeps a record of its processing activities in respect of personal data in accordance with the requirements of the GDPR.

6.5 Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);

- his/her rights to rectification or erasure of data, or to restrict or object to processing;

- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and,

- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

Inspire will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

If the individual wants additional copies, Inspire will charge a fee, which will be based on the administrative cost to Inspire of providing the additional copies.

To make a subject access request, the individual should send the request to the Data Protection Officer. In some cases, Inspire may need to ask for proof of identification before the request can be processed. Inspire will inform the individual if it needs to verify his/her identity and the documents it requires.

Inspire will normally respond to a request within a period of one month from the date it is received. In some cases, such as where Inspire processes large amounts of the individual's data, it may respond within three months of the date the request is received.
Inspire will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If a subject access request is manifestly unfounded or excessive, Inspire is not obliged to comply with it. Alternatively, Inspire can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Inspire has already responded. If an individual submits a request that is unfounded or excessive, Inspire will notify him/her that this is the case and whether or not it will respond to it.

Exemptions

The GDPR Bill contains exemptions to information that must be disclosed in response to a subject access request. These include where data is subject to legal professional privilege, is processed for the purpose of management planning, relates to intentions in negotiations with an individual, or consists of a confidential reference that the employer has given. Organisations may also redact or restrict disclosure where, for example, the information contains third-party personal data.

Keeping records of subject access requests

A record of a subject access request will be retained.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and,
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.
- To ask the organisation to take any of these steps, the individual should send the request to the Data Protection Officer.

6.6 Data security

Inspire takes the security of personal data seriously. Inspire has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Inspire's Information Security Policy & Procedures provides details about the controls in our systems, restrictions on access of data and how the risk of a security breach is minimised. Our policies describing the use of the Internet and Social Media and are linked to Bexley Council's procedures since Inspire's ICT systems are maintained under contract with them.

If Inspire engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

6.7 Impact assessments

Some of the processing that Inspire carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, Inspire will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

6.8 Data breaches

If Inspire discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. Inspire will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

6.9 International data transfers

Inspire will not transfer personal data to countries outside the EEA.

6.10 Individual responsibilities

Individuals are responsible for helping Inspire keep their personal data up to date. Individuals should let Inspire know if data provided to them changes, for example if an employee moves house or changes his/her bank details.

Individuals may have access to the personal data of other individuals and of our service users and relatives in the course of their work. Where this is the case, Inspire relies on individuals to help meet its data protection obligations to employees, service users, relatives, contractors and any others affected and protected by the GDPR.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from Inspire's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and,
- not to store personal data on local drives or on personal devices that are used for work purposes.

Further details about Inspire's security procedures can be found in it's the Information Security Policy & Procedures which describes the controls and restrictions for the use of the ICT system, email, internet, social media and smart/mobile phones.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under Inspire's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

6.11 Training and Instruction

Inspire will provide training and/or instruction to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.