Compliance Officer for
IPSA

Data Protection Policy

1. Purpose

1.1 The IPSA Compliance Officer (''the Compliance Officer'') is required by law to comply with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018).

1.2 The Compliance Officer needs to process certain personal information about individuals, to meet legal obligations. Such data must only be processed in accordance with this policy and the Compliance Officer's Records of Processing Activities, which sets out the purposes for which the personal data is processed.

2. Background

2.1 The General Data Protection Regulation (GDPR), establishes a framework of rights and duties which are designed to protect personal data. This is underpinned by a set of six principles which define how data can be legally processed.

2.2 These six principles are:

(a) Personal data shall be processed fairly, lawfully and transparently.
(b) Personal data shall be held only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.
(c) Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
(d) Personal data shall be accurate and where necessary kept up to date.
(e) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
(f) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of the data.

2.3 The GDPR also sets out rights of data subjects relating to their personal data. These rights include:

(a) the right of access
(b) the right to rectification
(c) the right to erasure (in certain circumstances)
(d) the right to stop processing
(e) the right to data portability (in certain circumstances)
(f) the right to object; and
(g) the right to prevent automated processing, including profiling

2.4 Definitions

2.4.1 *Processing* covers collection, recording, organisation, structuring, holding, retrieving, use, amending, disclosing, destroying of data, etc. Every organisation that holds any personal data about another individual in some form (hard copy or electronic) from where it can be retrieved is 'processing' data.

2.4.2 *Personal Data* is defined as any information relating to an identified or identifiable person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, or to one or more factors specific to an individual.

2.4.3 *Special Category Personal Data* is defined as personal data revealing:

(a) the racial or ethnic origin of a person
(b) the political opinions of a person
(c) the religious or philosophical beliefs of a person
(d) whether a person is a member of a trade union
(e) the physical or mental health or condition of a person
(f) the sexual life or sexual orientation of a person
(g) genetic, biometric data processed for the purpose of uniquely identifying a person

2.5 *Data Subject* is the living individual to whom the personal data relates.

2.6 *Data Controller* is the entity which, alone or jointly with others, determines the purposes for which and the means by which any personal data are, or are to be, processed. The Compliance Officer is the Data Controller under the GDPR.

2.7 *Data Processor* is any third party who processes personal data on behalf of the Data Controller. There will be written agreements with Data Processors to ensure they comply with the GDPR.

2.8 The GDPR sets out certain lawful bases that must be satisfied to justify the holding or use of personal data. These are set out in Article 6 of the GDPR and include:

(a) Consent of the data subject;
(b) Fulfilment of a contract;
(c) Fulfilment of a legal obligation;
(d) Protecting the vital interests of the data subject;
(e) Processing personal data in accordance with the Public Task; and
(f) Processing in accordance with the legitimate interests of the organisation.

2.9 In addition to this, where Sensitive Personal Data is processed, then in accordance with Article 9 GDPR, an additional processing condition will apply.

3. Responsibilities of the Compliance Officer

3.1 In order to process personal data, the Compliance Officer shall ensure that a condition from Article 6 (and Article 9, as applicable) of the GDPR is met.

3.2 All data shall be processed in a secure manner, and shall be stored securely, to prevent any loss, damage or unauthorised disclosure to a third party, either accidentally or otherwise.

4. Data Subjects' Rights

4.1 The Compliance Officer will endeavour to comply with any requests made to it by Data Subjects exercising any of these as they apply to the particular processing concerned, under the terms laid out in the GDPR. Data subjects may exercise their rights by informing the Compliance Officer in writing (subject to any reasonable adjustments being made, in accordance with relevant Equality Legislation).

5. Third Party disclosure

5.1 There are circumstances (known as exemptions), provided for under DPA 2018, where personal data may be disclosed to third parties without the consent of the Data Subject.

5.2 Any such disclosures will take place only if the Compliance Officer is satisfied that the party seeking this has provided written evidence of their entitlement to request this information and provided relevant justifications as required.

6. Records Management

6.1 Regardless of format, personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Some information may be retained for longer periods.

6.2 Information shall be retained in accordance with the Records Retention Policy and associated Records Retention Schedule and disposed of securely at the end of retention.

7. Review

7.1 This policy will be reviewed annually, or where there are any significant changes to legislation, updates to case law and/or additional or revised guidance issued by the Information Commissioner's Office.

Annex A – Checklist for processing personal data

When processing personal data, the following considerations will be taken into account:

(a) Are the purposes for processing justified?

(b) Is the personal data 'standard' or 'special category'?

(c) What condition(s) for lawfulness of processing is/are being relied upon?

(d) Has the Data Subject been informed that their data will be processed, and the purposes for this?

(e) Has the Data Subject been informed of his/her rights for e.g. by way of Privacy Notice?

(f) Will the data be securely held and who will have access?

(g) Who will the data be shared with?

(h) How long does the data need to be kept for and are there arrangements for its review or secure disposal?