POLICY STATEMENT

4i Solutions collects and processes personal and sensitive personal data from our service users and other stakeholders. As such we have a duty of care and an obligation under the law to treat the data we collect with care and in line with the rights of those data subjects.

1. SCOPE

1.1. This policy covers all usage of personal data information assets.

2. PRINCIPLES

2.1. 4i Solutions will adhere to both the letter and the spirit of relevant current Data Protection legislation as outlined in appendix B.

2.2. 4i Solutions will create and maintain suitable policies and procedures to ensure compliance.

2.3. 4i Solutions will ensure that all staff receive appropriate Information Security and Data Protection training. That training to be refreshed on an annual basis.

2.4. 4i Solutions will ensure that information is stored, processed and maintained in a secure manner in line with current best practice.

2.5. 4i Solutions will take active steps to highlight our service users and stakeholders rights under the legislation.

3. AIMS AND OUTCOMES

3.1. Safety and Security of data

3.1.1. 4i Solutions will actively pursue the safety and security of data, from a technical perspective as well as from a user and usage perspective.

3.2. Accuracy of data

3.2.1. 4i Solutions will use our best endeavours to ensure that the data we hold is accurate and up to date.

3.2.2. 4i Solutions will correct any inaccurate data as soon as we are aware of any inaccuracy and will take steps to ensure that inaccurate data is corrected on any data shared with any third party.

3.3. Subject Access Requests, Subject rights

3.3.1. 4i Solutions will respond to subject access requests in a timely manner in line with the data subject's rights under the legislation and in line with our Subject Access procedure.

3.4. Data Breaches and Reporting

3.4.1. 4i Solutions will report data breaches in a timely manner in line with our responsibilities under the legislation and in line with our Data Breach procedure.

3.4.2. 4i Solutions will investigate any data breaches and review policies and procedures in the light of the learning from that investigation.

3.5. Privacy Impact Assessments

3.5.1. All initiatives or changes requiring the collection of personal data will be subject to a privacy impact assessment in line with our Privacy Impact Assessment procedure.

3.6. Data Minimisation

3.6.1. 4i Solutions will only collect personal data where we have a legal basis for processing and will document that legal basis.

3.6.2. 4i Solutions will remove any personal data previously collected where we cannot substantiate a legal basis for processing.

3.7. Data Retention

3.7.1. 4i Solutions will only retain personal data where we have a legal basis for processing, in line with our data retention policy, or where we have a legal obligation to retain that data.

3.7.2. Data held beyond the retention period will be anonymised.

3.8. Personal data will only be shared with third parties:-

3.8.1. Where we have a legal basis for processing and where there is a written data protection agreement between the parties.

3.8.2. Where there is a legal requirement to share (e.g. with HMRC in order to satisfy taxation legislation on behalf of our employees.)

3.8.3. Where we have explicit, written consent of the data subject.

3.9. Data protection training

3.9.1. 4i Solutions will train staff in our collective and corporate responsibilities under data protection legislation.

3.9.2. We will train 4i Solutions staff to recognise and report a data breach in line with the relevant procedure.

3.9.3. That training to be documented and refreshed on an annual basis.

3.10. Data Protection roles and responsibilities

3.10.1. 4i Solutions will appoint a suitable officer to fulfil the role of Data Controller and to own Data Protection compliance within the organisation.

3.10.2. 4i Solutions are not required to appoint a Statutory Data Protection Officer.

4. DEFINITIONS

4.1. See appendix A.

5. STATUTORY AND REGULATORY REQUIREMENTS

5.1. See Appendix B - Principles of GDPR, Appendix C - Legal basis for processing data and Appendix D - Mandatory requirements under GDPR

6. REVIEW

6.1. This policy will be reviewed every two years, or in the light of any material change in data protection legislation or following any investigation of a notifiable breach.

Appendix A – Definitions

Data means information which –

(a) Is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) Is recorded with the intention that it should be processed by means of such equipment,
(c) Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) Does not fall within paragraph (a), (b) or (c) but forms part of an accessible record (health record, education record, local authority record),
(e) Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Data subject means an individual who is the subject of personal data.

Personal data means data which relate to a living individual who can be identified –

(a) From those data, or
(b) From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

Sensitive personal data means personal data consisting of information as to -

(a) The racial or ethnic origin of the data subject,
(b) Their political opinions,
(c) Their religious beliefs or other beliefs of a similar nature,
(d) Whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) Their physical or mental health or condition,
(f) Their sexual life,
(g) The commission or alleged commission by them of any offence, or
(h) Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Appendix B - Principles of GDPR

That personal data be:-

1 processed lawfully, fairly and in a transparent manner in relation to individuals

2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

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, using appropriate technical or organisational measures

The regulation requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Appendix C - Legal basis for processing data

The individual whom the personal data is about has consented to the processing.

The processing is necessary:

- in relation to a contract which the individual has entered into; or
- because the individual has asked for something to be done so they can enter into a contract.

The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).

The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.

The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions

The processing is in accordance with the "legitimate interests" condition.

Appendix D - Mandatory requirements under GDPR

1 To produce Privacy Impact Assessments – a risk assessment evaluating the use of data in projects

2 To have the policy and procedures in place to define how staff and anyone who processes data on our behalf behave in regard to data protection.

3 To be able to demonstrate that we are compliant with GDPR, and carry out periodic compliance checks reporting back to board.

4 To report data breaches to the ICO within 72 hours of their detection.

5 To ensure personal data are available, that systems are resilient, and that data can be restored in the event of an incident or loss

6 For someone to fulfil the statutory role of Data Protection Officer, a senior person, with detailed knowledge of GDPR. They must be independent, with no conflict of interest between the requirements of GDPR and any other duties they may fulfil. They may not be subject to undue influence in the fulfilment of their duties, and will report directly to the board on all matters related to GDPR

7 The European working party on GDPR said in the “Guidelines on Data Protection Officers (‘DPOs’)” regarding conflict of interest
“As a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing”