Policy: Data Protection

Department: IT

Date: **Approved October 2016** **Review Date:** **January 2018**

1.0 Purpose

This policy defines how 110% Ltd ensures its compliance to the latest Data Protection regulations as dictated and policed by the Information Commissioners Office (ICO).

2.0 Scope

This policy applies to:

- All personal data held and processed by 110% Ltd.
- All employees of 110% Ltd who are granted access to personal data.
- All contractors, suppliers, 110% Ltd partners and external collaborators and visitors who may be authorised to access 110% Ltd held personal data.
- All locations from which personal data is accessed including home and off-site/ remote use.
- Any other parties who may be holding personal data on behalf of 110% Ltd.

2.0 Legislation

There are several sets of legislation which impact on the way in which 110% Ltd manages information. Non-compliance with this legislation carries financial and reputational penalties for 110% Ltd. 110% Ltd needs to hold and to process large amounts of personal data about its employees, customers, contractors and other individuals in order to carry out its business.

Personal data is data which relates to a living individual, who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, 110% Ltd. Some types of personal data are more confidential than others, for example, details of a person's physical health or mental condition, and such data is known as sensitive personal data.

All personal data is subject to the Data Protection Act 1998, and 110% Ltd must ensure that it complies with the provisions of the Act. The Information Commissioner's Office (ICO) is the regulatory body which enforces compliance with the Act. Its powers include the power to fine for breaches of the Act. Further acts such as the Freedom of Information Act 2000 have further affected this legislation.

3.0 Key principles

Compliance with the Act will be achieved through the implementation of controls and responsibilities including measures to ensure that the eight core principles are followed:

1. Personal data is processed fairly and lawfully.
2. Personal data is processed only for the purposes for which it was collected.
3. Personal data is adequate, relevant and not excessive for the purposes for which it was collected.
4. Personal data is accurate and up to date.
5. Personal data is not kept for longer than necessary & disposed of securely when no longer required.
6. Personal data is processed in accordance with the rights of individuals under the Act.
7. Personal data is kept securely and appropriately. This includes both physical and digital media.
8. Personal data is not transferred outside of the EEA without adequate protection.

Measures will also be applied to ensure that sensitive personal data is handled appropriately by 110% Ltd. Sensitive personal data is defined as including information relating to an individual's: racial or ethnic origin; political opinions; religious or similar beliefs; trade union membership; physical or mental health or condition; sexual life; commission of offences and/or criminal proceedings.

4.0 Processing

The organisation will only process personal data in accordance with the requirements of data protection legislation. Personal or confidential information will only be disclosed or shared where an employee has been authorised to do so.

The Data Protection Act operates on the basic principle that a data processing operation (collecting data, storing it, or disclosing it) must have one of a series of possible justifications, which are set out in the Act. Other legislation may also be involved, and the Data Protection Act defines how this interface is to be managed.

It is important to note that merely retaining data, constitutes "processing" and therefore requires legal justification and compliance with the Data Protection Principles. Unless special arrangements are approved by the Data Protection Officer, all documents, files and records must be stored in approved locations. Approved locations are network drives and servers, and secure physical locations on site in regards to hard copy files.

For those involved in the storing of personal data it is their responsibility to ensure they are cognisant of the latest legislation and comply with the legislation at all times. Any concerns they may have should be escalated to their line manager for appropriate action. Line managers should then report to the Data Protection Officer if further advice is needed.

5.0 ICO Notification

Organisations processing personal data are required to register as a data controller with the Information Commissioner. This Notification describes the classes of personal data that are processed along with the purposes for processing. It applies to all personal data that is generated in the course of the Company's business regardless of where the data is physically stored.

Within the Data Protection Act there are both general requirements which affect all processing of personal data.
It is likely that some requests under the Freedom of Information Act for information will relate to personal data. Please see the Staff Privacy Notice and the Client Privacy Notice.

Data for which 110% Ltd is responsible includes:

The 110% Ltd Company Notification is based on a model Notification developed for the UK higher education sector and can be found (by typing in '110 Percent Group' against 'Name', then clicking 'Search') in the online national register. Data belonging to the Company - whether it be administrative data, or operational data which staff or partners have collected in the course of employment or contract with the Company - falls within the Company's Notification regardless of whether it is processed on Company premises or using Company computing facilities.

Activities carried out by members of the Company at home, or when travelling with a laptop, may therefore fall under the Company Notification; conversely some processing carried out on Company premises will be the responsibility solely of the individual concerned, or of another organisation (see below).

Data for which the Company is not responsible includes:

The following categories of data are excluded from the Company Notification:

- Personal data for personal and domestic use held and processed by staff and contractors - even if it is done using Company computing facilities. Notification is not required for this type of processing.
- Personal data processed in the course of a member of staff's activities not directly related to their employment with the Company, and where this activity is likely to lead to commercial exploitation. It is not normally appropriate for such activities to be carried out using Company computing facilities without special arrangements being made.
- Personal data processed on behalf of another organisation with which a member of staff or student is associated in a private capacity or in the course of wider professional activities (e.g. community group, conference for a professional body and trade union activities) - even if it is done using Company computing facilities. Such processing will most likely need to be covered by the outside organisation's Notification. Staff and consultants undertaking the processing should satisfy themselves that the appropriate Notification has been made, as the Company cannot accept responsibility for unlawful processing of data which is not under its control.
- Notification arrangements for organisations with which the Company is closely associated but have their own Notification under the Data Protection Act which is independent of the Company's.

This list of Notifications is not exhaustive. If you have any questions, please contact the Data Protection Officer.

6.0 Responsibility & Compliance

Heads of Department are responsible for ensuring that all staff and consultants within their area act in accordance with this policy. They are also responsible for ensuring that records are destroyed according to the retention schedule on an annual basis.

All staff have a responsibility to make informed decisions to protect and to properly manage personal data. Staff and other approved users of 110% Ltd must:

- All of our employees receive information security and privacy training. Employees that handle data receive additional training specific to their roles.
- Demonstrate competence in their understanding of data protection laws and good practice applicable to the performance of their 110% Ltd responsibilities and must seek advice and guidance if clarification is required.

- Report any actual or suspected breach in personal data security, “near misses” or working practices which jeopardise the security of personal data held by 110% Ltd.
- Not tamper or destroy any records that are subject to a data subject access request (DSAR).
- Follow the Off-site Processing procedures, 3rd Party Disclosures procedures and Data Subject Access Requests procedures.

Compliance with this policy is mandatory and non-compliance must be reported to the Data Protection Officer to record the incidence and escalate to the appropriate authority to determine the action to be taken. Noncompliance with this policy is subject to 110% Ltd.’s disciplinary procedures for staff and students.

7.0 Monitoring and auditing

This policy and its implementation will be subject to internal monitoring and auditing throughout the 110% Ltd, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. 110% Ltd will also undertake appropriate benchmarking and external auditing exercises.

8.0 Associated documents

Please refer to:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Freedom of Information Policy
- Staff Privacy Notice
- Client Privacy Notice
- Personal Data Request procedures
- Data Retention and Archiving Policy

9.0 Review of policy

This policy will be reviewed at least every two years or when there are significant changes to it.

10.0 Contact list for queries related to this policy

Data Protection Officer
Chief Information Officer

11.0 Authority for this policy

Senior Management Team