Tel: 0141 630 1323
Email: mail@jenniburn.co.uk
Web: jenniburn.eu
Twitter: @jenniburn

The Jenniburn Centre SCIO
370 Tormusk Road
Glasgow
G45 0HE

Data Protection Policy (GDPR)

1. ABOUT THIS POLICY

1.1 The Jenniburn Centre SCIO *(the organisation)* is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out our commitment to data protection, and individual rights and obligations in relation to personal data.

1.2 This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

1.3 The organisation has designated the Coordinator as the person will take responsibility for ensuring compliance. His/her contact details are as given above.

He/she has responsibility for data protection compliance within the organisation. Questions about this policy, or requests for further information, should be directed to the Coordinator.

1.4 This policy does not form part of the contract of employment and may be amended at any time.

1.5 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with your Line Manager.

2. DEFINITIONS

2.1 **"Personal data"** is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

2.2 **"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.

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

3. DATA PROTECTION PRINCIPLES

3.1 The organisation processes HR-related personal data in accordance with the following data protection principles:

- We process personal data lawfully, fairly and in a transparent manner.
- We collect personal data only for specified, explicit and legitimate purposes.
- We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- We keep accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

- We keep personal data only for the period necessary for processing.
- We adopt appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

3.2 We tell individuals the reasons for processing their personal data, how we use such data and the legal basis for processing in its privacy notices. We will not process personal data of individuals for other reasons.

3.3 Where the organisation 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.

3.4 We will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

3.5 Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship, is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the organisation holds HR-related personal data are contained in its privacy notices to individuals.

3.6 We keep a record of our processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

4. INDIVIDUAL RIGHTS

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

4.2 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.

4.3 We 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.

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

4.5 To make a subject access request, the individual should send the request to the Coordinator. In some cases, the organisation may need to ask for proof of identification before the request can be processed. We will inform the individual if we need to verify his/her identity and the documents we require.

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

4.7 If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation 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 organisation has already responded. If an individual submits a request that is unfounded or excessive, we will notify him/her that this is the case and whether or not we will respond to it.

5. OTHER RIGHTS

5.1 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

5.2 To ask the organisation to take any of these steps, the individual should send the request to the Coordinator.

6. DATA SECURITY[1]

6.1 We take the security of HR-related personal data seriously. We have 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 or Trustees in the proper performance of their duties.

6.2 Where the organisation 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.

7. IMPACT ASSESSMENTS

7.1 Some of the processing that the organisation carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, we 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.

8. DATA BREACHES

8.1 If the organisation discovers that there has been a breach of HR-related personal data that poses a significant risk to the rights and freedoms of individuals, it will

[1] See also Appendix 1

report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

8.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, we 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.

9. INTERNATIONAL DATA TRANSFERS

9.1 We will not transfer HR-related personal data to countries outside the EEA.

10. INDIVIDUAL RESPONSIBILITIES

10.1 Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let us know if data provided to us changes, for example if an individual moves to a new house or changes his/her bank details.

10.2 Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the organisation relies on individuals to help meet our data protection obligations to staff, customers and clients.

10.3 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 the organisation'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.

10.4 Further details about the organisation's security procedures can be found in our Data Security policy.

10.5 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under our 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 summary dismissal.

Data Security Policy

We have put in place procedures and technologies to maintain the security of all our HR-related data, the data of our clients or other personal data that is processed for business purposes. Data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

This policy does not form part of any employee's contract of employment and may be amended at any time.

If you consider that this policy has not been followed you should raise the matter with your Line Manager.

Any breach of this policy will be taken seriously and may result in disciplinary action, up to and including summary dismissal.

DATA SECURITY

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed and that and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported.
- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal.** Paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.

Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Appendix 1.

Procedures for Handling Data and Data Security

The Board of Trustees has a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

Unauthorised or unlawful processing of personal data:

Unauthorised disclosure of personal information classed as personal data and falls within the scope of the DPA. It is therefore important that all staff consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below.

Privacy Notice and Consent Policy

The private notice and consent policy are as follows: Consent forms will be stored by the Secretary in a securely held electronic or paper file. Operational Guidance Email

All trustees, staff and volunteers should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or printed and stored securely.

Remember, emails that contain personal information no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Phone Calls Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- Personal information should not be given out over the telephone unless you have no doubts as to the caller's identity and the information requested is innocuous.
- If you have any doubts, ask the caller to put their enquiry in writing.
- If you receive a phone call asking for personal information to be checked or confirmed be aware that the call may come from someone impersonating someone with a right of access. Laptop/tablet/smartphone/tablet/smartphones and Portable Devices
- All laptop/tablet/smartphones and portable devices that hold data containing personal information must be protected with a suitable encryption program (password).
- Ensure your laptop/tablet/smartphone is locked (password protected) when left unattended, even for short periods of time.
- When travelling in a car, make sure the laptop/tablet/smartphone is out of sight, preferably in the boot. The Centre Data Protection Policy 5
- If you have to leave your laptop/tablet/smartphone in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.
- Never leave laptop/tablet/smartphone or portable devices in your vehicle overnight.
- Do not leave laptop/tablet/smartphone or portable devices unattended in restaurants or bars, or any other venue.
- When travelling on public transport, always keep it with you. Do not leave it in luggage racks or even on the floor alongside you.

Data Security and Storage

Store only the minimum amount of personal data required on the laptop/tablet/smartphone/tablet/smartphone and only keep those files that are essential.

Personal data received on disk or memory stick should be saved to the relevant file on the server or laptop/tablet/smartphone/tablet/smartphone

The disk or memory stick should then be securely returned *(if applicable)*, safely stored or wiped and securely disposed of. Always lock (*password protect*) your computer or laptop/tablet/smartphone/tablet/smartphone when left unattended.

- Passwords[2] Do not use passwords that are easy to guess.
  All your passwords should contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.
  Protect Your Password:
- Common sense rules for passwords include not giving out your password(s) to anyone, not writing your password somewhere in or on your laptop/tablet/smartphone
- Information should be stored for only as long as it is needed or required by statute and then disposed of appropriately.
- Archival material such as minutes and legal documents will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required or when trustees, staff or volunteers retire.
- Appropriate steps must be taken to ensure that all personal data held for the organisation must be non-recoverable from any computer which has been passed on/sold to a third party.

[2] The Jenniburn Centre SCIO uses password manager software to securely encrypt such data to a high level.