Data Protection Policy

Date of Policy Approval:

Due Date for Review of Policy:

Contents

1. Introduction

This policy applies to all our employees, board members and volunteers.

The purpose of this policy is to enable STC Careers to:

- comply with the law in respect of the data it holds about individuals
- follow good practice
- protect STC Careers' supporters, staff and other individuals
- protect the organisation from the consequences of a breach of its responsibilities

The General Data Protection Regulations 2018 regulates the processing of information relating to living and identifiable individuals (data subjects). This includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

Data users must comply with the data protection principles of good practice which underpin the General Data Protection Regulations and best practice for Information Governance and Data Security and Protection.

Personal data must be:

- obtained and processed fairly and lawfully
- held only for specified purpose
- adequate, relevant and not excessive
- accurate and up to date
- not kept longer than necessary
- processed in accordance with the Regulations
- kept secure and protected
- not transferred to countries without adequate data protection

STC Careers holds two types of information:

- Personal information – information held about individuals such as names, addresses, job titles
- Sensitive personal information – information held about employees such as health and disability; and clients such as information about health and disability, safeguarding procedures etc.

This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the General Data Protection Regulations, by virtue of not meeting the strict definition of “data” in the Regulations.

STC Careers has identified the following potential key risks, which this policy is designed to address:

- breach of confidentiality (information being given out inappropriately)
- insufficient clarity about the range of uses to which data will be put – leading to Data Subjects being insufficiently informed
- failure to offer choice about data use when appropriate
- breach of security by allowing unauthorised access
- failure to establish efficient systems of managing changes to our staff and volunteers, leading to personal data being not up to date
- harm to individuals if personal data is not up to date
- insufficient clarity and failure to offer choice about how personal data of staff and volunteers and others is used
- data protection issues in partnerships and other collaborative relationships
- data protection issues in relation to contractors and other external bodies
- data processor contracts

2. Policy Statement

STC Careers will:

- comply with both the law and good practice
- respect individuals’ rights
- be open and honest with individuals whose data is held
- provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently

STC Careers recognises that its first priority under the General Data Protection Regulations is to avoid causing harm to individuals. In the main this means:

- keeping information securely in the right hands, and
- holding good quality information

Secondly, the Regulations aim to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, STC Careers will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

3. Responsibilities

Board members

The board recognises its overall responsibility for ensuring that STC Careers complies with its legal obligations.

Data Protection Adviser

The Data Protection Adviser is currently Elizabeth Harding-Massey, ehardingmassey@gmail.com, 07912064416 who has the following responsibilities:

- briefing the board on data protection responsibilities
- reviewing data protection and related policies
- advising other staff on data protection issues
- ensuring that data protection induction and training takes place
- reporting data breaches to the Information Commissioners Office
- handling subject access requests
- approving unusual or controversial disclosures of personal data
- approving contracts with data processors
- ensuring signed written agreements are in place between the data Controller and the data Processors and these have appropriate data protection clauses;
- electronic security;
- ensuring that all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been disposed of or passed on/sold to a third party.
- approving data protection-related statements on publicity materials and letters

Each employee, board member and volunteer who handles personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good Data Protection practice is established and followed. All employees, board members and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy and breach of personal data may be handled under our disciplinary procedures.

4. Confidentiality

In order to provide some services, we will need to share client's personal data with other agencies (Third Parties). Verbal or written consent will always be sought from the client before data is shared.

Where anyone within our organisation feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done after discussions with a manager or the Data Protection Adviser (Elizabeth Harding-Massey, ehardingmassey@gmail.com, 07912064416). All such disclosures will be documented.

5. Security

This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

Any recorded information on clients, volunteers and employees will be:

- Handled, transferred, processed and stored with the up-most care and regard.
- When not being handled, transferred or processed, it will be stored in secure office facilities, locked drawers or cabinets, or secure cloud-based digital storage.
- Protected by the use of passwords if kept on computers and/or other devices and encrypted if appropriate.
- Destroyed confidentially if it is no longer needed, or if an individual requests.

Access to information on the main database and/or cloud based facilities is controlled by a password and only those needing access are given the password. Employees, board members and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display.

Paper files will be stored in a secure location, with controlled access to authorised personnel only.

Notes regarding personal data of clients should be shredded or destroyed.

6. Data recording and storage

We use secure cloud-based systems for holding basic information about all staff, clients and volunteers. The back-up copies of data are kept in a safe place.

We will regularly review our procedures for ensuring that our records remain accurate and consistent and, in particular:

- We will keep records of how and when information was collected.
- The storage system is reviewed and re-designed, where necessary, to encourage and facilitate the entry of accurate data.
- All employees, board members and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes.
- Effective procedures are also in place to address requests from Data Subjects for access to, amendments or the erasure of their information
- Employees, board members and volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping in compliance with the GDPR.
- Data will be corrected if shown to be inaccurate or a request is made by a Data Subject.

We store archived paper records of clients and volunteers securely in the office.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

7. Data breach

All Staff, board members and volunteers are required to report any data breach to the Data Protection Adviser, Elizabeth Harding-Massey, ehardingmassey@gmail.com, 07912064416) as soon as possible once they are aware it has occurred. A data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data transmitted, stored or otherwise processed.

The Data Controller is responsible for recording and reporting any data breaches that occur across the organisation.

Less serious breaches will be recorded and listed in an appropriate place, and trends or lessons learned will be reviewed.

Serious personal data breaches will be reported by the Data Protection Adviser Elizabeth Harding-Massey, ehardingmassey@gmail.com, 07912064416) at the

earliest possible time, as well as reported to the ICO within 72 hours of the breach occurring if possible, and if not, informing the ICO the reasons for any delay.

Incidents that STC Careers may face that constitute a data breach:

- staff or volunteers loosing data in transit
- staff or volunteers with access to personal information miss using it
- staff tricked into giving away information, either about supporters or colleagues, especially over the phone
- staff or volunteers accidently sending personal information to the wrong person, especially by email
- STC Careers servers hacked and personal information falling it other people's hands or made accessible on line
- unauthorised access by staff and volunteers while working and no longer working for STC Careers

8. Access to data

Information and records will be stored securely and will only be accessible to authorised employees and volunteers, and the individual to whom the information relates.

All clients and customers have the right to request access to all information stored about them. Any subject access requests will be handled by the Data Protection Officer within the required time limit.

Subject access requests must be in writing or by email. All employees, board members and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay. In accordance with the GDPR, we will provide personal data in a 'commonly used and machine readable format.' We also recognise the right of the individual to transfer this information to another Controller.

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.

The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

We will provide details of information to clients who request it unless the information may cause harm to another person.

Employees have the right to access their file to ensure that information is being used fairly. If information held is inaccurate, the individual must notify the Manager so that this can be recorded on file.

9. Transparency

We are committed to ensuring that in principle Data Subjects are aware that their data is being processed and

- for what purpose it is being processed
- what types of disclosure are likely
- how to exercise their rights in relation to the data.

Data Subjects will generally be informed in the following ways:

- Employees: in the staff terms and conditions
- Volunteers: in the volunteer welcome/support pack
- Board members: in the roles and responsibilities/support pack
- Clients: when they provide their information and consent to retain it is requested, or when they request (on paper, online or by phone) services

Standard statements will be provided to all staff for use on forms where data is collected.

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

10. Consent

Staff details will only be disclosed for purposes unrelated to their work for the organisation (e.g. financial references) with their consent.

Information about volunteers will be made public according to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role.

Information about clients will only be made public with their explicit consent. (This includes photographs.)

‘Sensitive’ data about clients (including health information) will be held only with the knowledge and consent of the individual.

Consent should be given in writing, although for some services it is not always practicable to do so. In these cases verbal consent will always be sought to the storing and processing of data, and records kept of the dates, and circumstances. Online consent will be requested when clients sign up to services, donate or sign up to mailing lists. In all cases it will be documented on the database that consent has been given.

All Data Subjects will be given the opportunity to opt out of their data being used in particular ways, such as the right to opt out of direct marketing (see below).

We acknowledge that, once given, consent can be withdrawn by the Data Subject at any time. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

11. Direct marketing

We will treat the following unsolicited direct communication with individuals as marketing

- seeking donations and other financial support
- promoting any of our services
- promoting our events
- promoting membership to supporters
- promoting sponsored events and other fundraising exercises
- marketing on behalf of any other external company or voluntary organisation

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be asked to provide their consent. We do not have a policy of sharing lists, obtaining external lists or carrying out joint or reciprocal mailings.

We will only carry out telephone marketing where consent has been given in advance, or the number being called has been checked against the Telephone Preference Service.

12. Staff training and acceptance of responsibilities

All employees that have access to any kind of personal data will be given copies of all relevant policies and procedures during their induction process, including the Data Protection policy. All staff and volunteers will be expected to adhere to all these policies and procedures.

Data Protection will be included in the induction training for all volunteers.

We will provide opportunities for all staff and volunteers as appropriate to explore Data Protection issues through training, team meetings, and supervisions.

13. Definition of terms

Confidentiality
Confidential information is defined as verbal or written information, which is not meant for public or general knowledge, information that is regarded as personal by clients, board members, employees or volunteers.

Consent
Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data
One piece or a combination of information that relates to a person or a 'Data Subject' that could identify them, that is stored:

a) Electronically i.e. on computer, including word processing documents, emails, computer records, CCTV images, microfilmed documents, backed up files or databases, faxes and information recorded on telephone logging systems.
b) Manually i.e. records which are structured, accessible and form part of a filing system where individuals can be identified and personal data easily accessed without the need to trawl through a file.

Data concerning health
personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Data Controller
The person who (either alone or with others) decides what personal information we will hold and how it will be held or used.

Data Processor
A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

Data Protection Act 1998
The UK legislation that provides a framework for responsible behaviour by those using personal information, which will be superseded by the General Data Protection Regulations on 25 May 2018.

Data Subject
Any living individual whose personal data is being processed. Examples include:

- employees – current and past
- volunteers
- apprentices
- job applicants
- donors

- clients
- suppliers

‘Explicit’ consent
Freely given, specific and informed agreement by an individual to the processing of personal information about them, leaving nothing implied. Explicit consent is needed for processing sensitive data.

Information Commissioner
Person responsible for implementing and overseeing the General Data Protection Regulations.

Notification
Notifying the Information Commissioner about the data processing activities of STC Careers if required, however certain activities for not for profit organisations may be exempt from notification.

Personal data breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Processing
The use made of personal data including any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Data Protection Officer or Adviser
The person(s) responsible for ensuring that we follow our data protection policy and complies with the General Data Protection Regulations

Data Protection Officer
A qualified Data Protection officer is required by some organisations depending on the number of staff and if they process sensitive data. Every organisation is advised to check their own situation on the ICO website for guidance

Data Protection Adviser
For organisations who have checked their position as advised above and are sure they do not need a qualified Data Protection Officer we recommend that a Data Protection Adviser is appointed by every organisation to support the implementation of GDPR and be a central contact point e.g. for requests for personal data or the right to be forgotten

Sensitive Data

Factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person

Third Party agreements

Many organisations use third parties to store/process data such as: online payments, online forums, cloud storage facilities. There should be a third party written agreement with the other organisation to confirm they are meeting the regulations. These can sometimes be found as web based documents. The data needs to be stored on European servers to ensure they comply with GDPR

14. Appendix

Privacy Statement

STC CAREERS C.I.C, Unit 7-8, Delta Bank Road, Metro Riverside Park, Gateshead, United Kingdom, NE11 9DJ Company number

When you request information from us, sign up to any of our services or buy things from us, we obtain information about you. We will ask for your consent to retain this information, and make it clear what your information will be used for. This statement explains how we look after that information and what we do with it.

We have a legal duty under the General Data Protection Regulations to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant and not excessive.

Normally information we hold comes directly from you, as set out in our Data Protection Policy. Whenever we collect information from you, we will ask for your consent to collect this information and make it clear what the purpose of this collection is, for example; which information is required in order to provide you with the information, service or goods you need. You do not have to provide us with any additional information unless you choose to.

We store your information securely on our computer system, we restrict access to those who have a need to know, and we train our staff in handling the information securely.

If you have signed up to a training event or other service, when you sign up we will ask you for consent to pass your details to the professional worker/volunteer providing that service. That worker/volunteer may hold additional information about your participation in these activities. We have an agreement in place with our professional workers/volunteers or any other agents or sub-contractors which we need to disclose your personal information to our agents or sub-contractors. They will only able to use your personal information in accordance with this agreement. In addition, we may disclose your personal information if required to do so by law, in connection with any legal proceedings or prospective legal proceedings, and in order to establish, exercise or defend our legal rights.

We would also like to contact you in future to tell you about other services we provide, to keep you informed of what we are doing and ways in which you might like to support us. You have the right to ask us not to contact you in this way and to ask us to remove the information which we hold on you. We will always aim to provide a clear method for you to consent for your information to be stored for this purpose. You can also contact us directly at any time to tell us not to send you any future marketing material or to remove your information by contacting us at:

Email: elizabeth@stccareers.co.uk

Phone: 07912064416

You have the right to a copy of all the information we hold about you (apart from a very few things which we may be obliged to withhold because they concern other people as well as you).

To obtain a copy, either ask for an application form to be sent to you, or write to our Data Protection Adviser, Elizabeth Harding-Massey, at the address given above. We aim to reply as promptly as we can and, in any case, within the legal maximum of 30 days.

Updating This Statement

We may update this privacy policy by posting a new version on this website at any time. You should check this page occasionally to ensure you are familiar with any changes.

Other Websites

This website may contain links to other websites. We are not responsible for the privacy policies or practices of any third party.

Confidentiality statement for staff and volunteers

When working for STC Careers, you will often need to have access to confidential information which may include, for example

- personal information about individuals who are users of our services or otherwise involved in the activities organised by STC Careers
- information about the internal business of STC Careers
- personal information about colleagues working for STC Careers

STC Careersis committed to keeping this information confidential to protect people and STC Careers itself. ‘Confidential’ means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the General Data Protection Regulations, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by STC Careers to be made public, for example on the online database. Passing information between STC Careers and a mailing house, or vice versa does not count as making it public, but passing information to another organisation does count. You can share information about organisations where this information is already in the public realm, for example registered charities, but you should still be careful about information that can be linked to individuals (staff, volunteers, board members and clients) connected with organisations. This is also in line with the Information Governance requirements of the NHS.

You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- not compromise or seek to evade security measures (including computer passwords)
- be particularly careful when sending information outside the office
- not gossip about confidential information, either with colleagues or people outside STC Careers
- not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working for STC Careers.

I have read and understand the above statement. I accept my responsibilities regarding confidentiality.

Signed: Date: