# Data Protection Policy

St John's Centre collects, stores, uses and shares personal information about the people who come into contact with it, both directly from them, and sometimes from other people or organisations. We need to do this in order to carry out our work. However this information is vulnerable to abuse, and it is therefore important to deal with it according to safeguards provided by the EU General Data Protection Regulations 2018 (GDPR).

This Policy sets out the Centre's responsibilities for the personal information it deals with, and defines a framework for its compliance with the GDPR.

## Definitions

**Personal Information** – Information that relates to the identity of a natural person and can identify them directly or indirectly. It does not apply to information about companies and agencies.

**Processing -** the collection, recording, transmission and storing of personal information.

**GDPR** – The EU General Data Protection Regulations 2018, the EU legislation that provides the legal requirements for responsible behaviour by those processing personal information.

**Information Commissioner's Office (ICO)** – The Information Commissioner is responsible for implementing and overseeing the GDPR in the UK.

**Data Subject** – The individual whose personal information is being processed.

**Special categories of personal data** – data relating to:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

**Data Controller** – The person or organisation who (either alone or with others) decides what personal information the Centre will process and how it will be processed. The GDPR requires every data controller to register with the ICO, unless they are exempt.

**Data Processor** – a person or organisation responsible for processing personal data on behalf of a controller.

**Data Protection Officer** – the person responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements. This post is not required in all organisations.

**Personal data breach** - a breach of security (deliberate or accidental) leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

## Principles

**St John's Centre regards the lawful and correct treatment of personal information as essential to successful working, and to maintaining the confidence of the people and organisations that we deal with. St John's Centre will therefore ensure that personal information is treated lawfully and correctly.**

St John's Centre will adhere to the following Principles of Data Protection. These are based on the principles set out in the GDPR.

Personal information processed by the Centre :

- shall be processed lawfully, fairly and in a transparent manner in relation to individuals;
- shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purpose(s);
- shall be adequate, relevant and limited to what is necessary in relation to those purpose(s)
- shall be accurate and, where necessary, be kept up to date by all reasonable steps;
- shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of processing;
- shall be processed in accordance with the rights of data subjects under the GDPR; and
- shall be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures

## Data Processor and Data Controller

**St John's Centre is both a Data Processor and a Data Controller under the GDPR.** As a Data Controller, it is exempt from registration with the ICO because it does not process information automatically.

## Data Protection Officer

Under the GDPR, St John's Centre does not need to appoint a Data Protection Officer. **Christine Aspinall** is the member of staff responsible for data protection issues (the Data Protection Lead), and **Evelyn Cosham**?? is the Board member responsible.

The Data Protection Lead is the key point of contact for staff and other stakeholders in respect of Data Protection legislation.

## Data collection

St John's Centre will provide privacy information to individuals at the time it collects their personal data from them, in accordance with the GDPR. This applies to data that is collected verbally, in writing, or electronically.

This information will also be available at all times on the Centre website.

St John's Centre will, so far as is reasonably possible, ensure that the Data Subject is competent enough to give consent for processing, and has given so freely without any duress.

**Special Categories and Criminal Offence Data**

St John's Centre collects some Special Categories of personal data as part of its monitoring, some of which is required by funders. This is permitted under the GDPR because the data is necessary to ensure equality of opportunity or treatment. This data will be anonymised before it is shared or used in publicity.

As an employer, the Centre is also entitled to require disclosure of unspent criminal convictions by potential employees and volunteers, even if their role does not require a DBS check. The Centre fulfils the requirements of the GDPR regarding the collection and retention of this information.

## Data Storage

Personal information will be stored securely, whether in hard copy or electronically, and will only be accessible to authorised staff and volunteers.

Information will be stored for only as long as it is needed or required by statute, and will be disposed of responsibly when the need for retention ends.

St John's Centre will ensure all that all information is non-recoverable from any computer system previously used within the organisation, which has been passed on to a third party.

## Contact with Data Subjects

St John's Centre will only use personal information to contact data subjects for the purpose specified when the data is collected. Contact for any other purpose, for example general advertising of events at the Centre or elsewhere, will only occur if the subject has given separate consent for this.

## Data Sharing

St John's Centre may share data with other agencies such as learning providers, funding bodies and other voluntary agencies, with the consent of the data subject, if it will enable the Centre to provide a service to the subject.

There are circumstances where the law allows St John's Centre to disclose data (including special categories) without the data subject's consent. These are:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting vital interests of a data subject or other individual
- Sharing information which the data subject has already made public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion
- Providing a confidential service where the data subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

If a member of staff is uncertain whether these circumstances apply, they should consult the Data Protection Lead and the Centre Manager.

## Data Rights

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

St John's Centre will inform data subjects of their rights, and how they can exercise them, when it collects their data.

The Centre will deal promptly and courteously with any enquiries about handling personal information. This may be done by any suitable member of staff without reference to the Data Protection Lead, but if they are in any doubt, they should consult the Data Protection Lead before responding. A record of what information was requested and provided will be provided to the Data Protection Lead.

Information provided will be concise, transparent, intelligible, easily accessible, and it will use clear and plain language. It will be available to the subject verbally, in writing, or in any reasonable electronic format if requested by the data subject.

## Data Breaches

If a member of staff knows or suspects that a personal data breach has occurred, they will report it to the Data Protection Lead for investigation.

If it is concluded that a breach has occurred, the Data Protection Lead, in consultation with the staff involved, will establish the likelihood and severity of the resulting risk to people's rights and freedoms, and notify the ICO if necessary, based on the guidance in the GDPR. If it is decided that notification is not necessary, the decision, and the reasons for it, will be recorded.

In the case of a breach resulting in a high risk to the people's rights and freedoms, the Data Protection Lead will also inform the data subjects concerned as soon as possible, as set out in the GDPR.

Any security breach thought to be a consequence of criminal activity will also be reported to the Police and/or other National Security agency.

Following a confirmed breach, the Data Protection Lead, Board member responsible for Data Protection, and other staff will investigate whether any changes to policies, procedures or staff training are needed to prevent a similar breach occurring in future.

## Procedures

All Centre staff, and some volunteers, are involved in processing personal information. They all are individually responsible for following good data protection practice and complying with the requirements of this Policy.

St John's Centre will ensure that everyone processing personal information:

- is appropriately trained to do so, with training refreshed and updated as necessary;
- is properly resourced (given the necessary time, information and equipment, e.g. computer software);
- is appropriately supported by other staff and supervised by their Manager or Supervisor; and
- has read this policy as part of their induction process.

Significant breaches of this policy by paid staff will be dealt with under the Centre's Disciplinary Procedure. Breaches by volunteers will be dealt with under the Centre's volunteer procedures.

St John's Centre will:

- regularly review and audit the ways it processes personal information; and
- regularly assess and evaluate its performance in relation to handling personal information.

This Policy will be reviewed and updated as necessary to reflect best practice in data management, security and control, and to ensure compliance with any changes or amendments made to the GDPR, and any future guidance issued by the ICO.

Reviewed May 2018