St. Antony's Centre

General Data Protection Regulations (GDPR) Policy

1 Introduction and Background

1.1 St. Antony's Centre is a Data Controller and consequently must process all Personal Data (including Special Categories of Personal Data) about Data Subjects in accordance with the General Data Protection Regulation 2016/679 (the "GDPR") and any other relevant data protection legislation, domestic or otherwise, (as may be in force or repealed or replaced from time to time) (together the "Data Protection Rules").

1.2 St. Antony's Centre will collect, store, use and otherwise process Personal Data about the people with whom it interacts, who are the Data Subjects. This may include volunteers, trainees, clients, employees, contractors, suppliers and other third parties.

1.3 St. Antony's Centre processes Personal Data so that it can comply with its statutory obligations and achieve its charitable objects to meet the requirement of funding organisations both Public and Private to comply with other Government Legislation.

1.4 Every Data Subject has a number of rights in relation to how St. Antony's Centre processes their Personal Data. St. Antony's Centre is committed to ensuring that it processes Personal Data properly and securely in accordance with the Data Protection Rules, as such commitment constitutes good governance and is important for achieve and maintaining the trust and confidence of Data Subjects. St. Antony's Centre will regularly review its procedures to ensure that they are adequate and up-to-date.

1.5 All staff and volunteers of St. Antony's Centre who are involved in the Processing of Personal Data have a duty to protect the data that they process and must comply with this Policy. St. Antony's Centre will take any failure to comply with this Policy or the Data Protection Rules very seriously. Any such failure could result in legal action being taken against the Charity or the individual responsible.

2 The Data Protection Principles

2.1 St. Antony's Centre as the Data Controller is required to comply, and to demonstrate compliance, with the six data protection principles set out in the GDPR, which provide that Personal Data must be:

2.1.1 processed fairly, lawfully and in a transparent manner;

2.1.2 collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes;

2.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

2.1.4 accurate and, where necessary, kept up-to-date – every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay;

2.1.5 kept in form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed; and

2.1.6 processed in a way that ensures tis security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational security measures.

2.2 There is also an overarching principle; the Data Controller must be able to demonstrate compliance with the six principles. **Accountability** is vital.

3 St. Antony's Centre Data Protection Officer and Registration with the ICO

3.1 St. Antony's Centre Trustees have overall responsibility for compliance with the Data Protection Rules. However, the Data Protection Officer (the DPO) shall be responsible for ensuring day-to-day compliance with this Policy and with the Data Protection Rules. The DPO will undergo training at least once every 12 months and St. Antony's Centre will provide the DPO with sufficient resources and support to carry out their responsibilities. The DPO's name and contact details can be found in paragraph 10 of this Policy.

3.2 St. Antony's Centre is responsible for paying to the ICO any data protections fees levied on Data Controllers by the Data Protection Rules.

3.3 This Policy applies to all Personal Data processed by St. Antony's Centre in whatever format (e.g: paper, electronic, film) and regardless of how it is stored (e.g: electronically or in filing cabinets). It also includes information that is in paper form but is intended to be put into electronic form and to any recordings made such as taped recordings, CCTV footage or voice mail/messages.

4 How St. Antony's Centre will Comply and Demonstrate Compliance

4.1 This Policy is intended to ensure that any Processing of Personal Data is in accordance with the Data Protection Rules and the data protection principles. St. Antony's Centre will therefore:

4.1.1 ensure that, when personal information is collected (whether direct from the individual or from a third party), the Data Subject is provided with a Privacy Notice and informed of what data is being collected and for what legitimate purpose(s);

4.1.2 be transparent and fair in processing Personal Data;

4.1.3 take steps to ensure the accuracy of data at the point of collection and at regular intervals thereafter, including advising Data Subjects of their right to ask for rectification of Personal Data held about them;

4.1.4 securely dispose of inaccurate or out-of-date data, or data which is no longer required for the purpose(s) for which it was collected;

4.1.5 share information with others only when it is lawful to do so and ensure that individuals are informed of the categories of recipient to whom data will or may be disclosed and the purposes of any such disclosures;

4.1.6 ensure that additional safeguards (as required by the Data Protection Rules) are in place to protect Personal Data that is transferred outside of the European Economic Area (the "**EAA**") (see section 7.4 of this Policy);

4.1.7 ensure that data is processed in line with the Data Subject's rights, which include the right to:

(a) request access to Personal Data held about them by St. Antony's Centre (including, in some cases, having it provided to them in a commonly used and machine-readable format);

(b) have inaccurate Personal Data rectified;

(c) have the processing of their Personal Data restricted in certain circumstances;

(d) have Personal Data erased in certain specified situation (in essence where the continued processing of it does not comply with the Data Protection Rules);

(e) prevent the processing of Personal Data for direct-marketing purposes (which includes for fundraising and wealth screening purposes);

(f) as St. Antony's Centre to prevent Processing of Personal Data which is likely to cause unwarranted or substantial damage or distress to the Data Subject or any other individual; and

(g) prevent, in some cases, decisions being made about them which are based solely on automated processing (i.e: without human intervention) and which produce significant or legal effects on them;

(h) lodge a complaint with a supervisory authority, namely the Information Commissioner's Office (ICO)

4.1.8 ensure that only staff who have completed relevant GDPR training are permitted access to personal data, while staff responsible for submission of data to third parties such as prime contractors must first have completed any necessary data protection training as required by the third party;

4.1.9 ensure that all volunteers and employees are aware of St. Antony's Centre's data protection policies and procedures and their own responsibilities in terms of data protection, and understand that failure to comply may result in disciplinary sanctions in the event of non-adherence or breach; and

4.1.10 adopt, monitor and keep under review, a data retention schedule which sets out the periods for which different categories of Personal Data will be kept.

4.2 Through adherence to this Policy and related data protection policies, and through appropriate record-keeping, St. Antony's Centre will seek to demonstrate full compliance with each of the data protection principles.

4.3 In addition, the Data Protection Rules require the Data Controller to carry out a Data Protection Impact Assessment (a **"DPIA"**) prior to undertaking any Processing of Personal Data that is likely to result in a high risk for the rights and freedoms" of individuals. DPIAs will therefore be considered where appropriate in relation to the implementation of any new projects, services or systems which could result in a high privacy risk to individuals (particularly where new technology is being deployed) and will consider other regulation relevant to data protection, such as the Privacy and Electronic Communications Regulations. Please contact the DPO for guidance (see paragraph 10 of this Policy).

5 Data Security and Responsibilities of Staff and Volunteers

5.1 St. Antony's Centre shall ensure that appropriate technical and organizational security measures are in place to prevent unauthorized or unlawful Processing or damage to or loss (accidental or otherwise), theft, or unauthorised disclosure of Personal Data (a "Data Breach"). In particular, all staff and volunteers should ensure that:

5.1.1 the only individuals who have access to Personal Data and are able to process it are those who are authorised to do so;

5.1.2 Personal Data is stored only on the central St. Antony's Centre computer system and not on individual PCs, portable electronic devices or removable storage media, unless those devices are approved in advance and compliant with St. Antony's Centre's Policy and in all cases, they are subject to appropriate measures of password protection, encryption and deletion;

5.1.3 passwords are kept confidential, are changed regularly and are not shared between anyone other than the Data Protection Officer and/or Director as may be required;

5.1.4 any personal data transmitted electronically is password protected, with the password to open any documents sent by separate correspondence;

5.1.5 PCs are locked or logged off and paper documents are securely locked away when individuals are away from their desks;

5.1.6 Offices, desks and filing cabinets/cupboards are kept locked if they contain Personal Data of any kind, whether in digital or electronic format or on paper;

5.1.7 When destroying Personal Data, paper documents are securely shredded and electronic data is securely deleted in line with the Policy and guidance issued;

5.1.8 Paper or electronic records containing personal data may only be removed from the Centre premises for mobile or home working in exceptional circumstances and with the prior authorisation of the Data Protection Officer. When working from home or on an outreach basis staff and volunteers are required to log in remotely to the Centre's secure network and are not permitted to open or move documents containing personal data outside of the network (e.g. on a laptop desktop or hard drive).

5.1.9 Personal Data removed from a secure area is subject to appropriate security measures, including keeping paper files in a place where they are not visible or accessible by the public; using passwords/passcodes; encrypting portable electronic devices or storing such devices securely (e.g.: not left in the boot of a car overnight);

5.2 In the event that you become aware that there has been a Data Breach, you must report this immediately to the DPO following the Data Breach Procedure, to the Director kflanagan@stantonyscentre.org.uk. Further contact details for the DPO can be found in paragraph 10 of this Policy.

6 Staff Induction and Training

6.1 At induction, new staff are provided with a copy of the Centre's GDPR Policy and are required to sign and return a statement confirming their understanding of the procedures and protocols for Data Protection within 2 weeks of starting their employment. Alongside the hard copy of the

Policy, an electronic version is held on a shared Policy folder on the Centre server to which all staff have access, with staff instructed by email of any changes to the policy.

6.2 At induction, new staff are issued with discrete usernames and passwords in order to access the Centre server and made aware that disclosure of their password other than to the Data Protection Officer and/or Director will lead to disciplinary action up to and including dismissal. The Data Protection Officer is responsible for allocating permissions against each username and password which limit access to areas of the Centre network and server the member of staff requires to undertake their duties.

6.3 Following induction all staff with access to personal data are required to complete mandatory GDPR training within one month of their start date and must pass this training before being granted access to such data. In the event that a new member of staff does not pass the training, additional one-to-one support will be provided by the Data Protection Officer to embed understanding of the principles and practice of data protection.

6.4 All staff are required to undertake formal refresher training in GDPR as a minimum every 2 years or immediately in response to changes in data protection legislation. This is underpinned by email updates and formal briefings, including policy changes, from the Data Protection Officer as part of annual training and development sessions held with all staff in January.

6.5 Centre servers and systems are subject to Cyber Essential Plus testing annually by an external agency to ensure safety of computer and remote systems and best practice in meeting the standards required. Current assessments are conducted by Bulletproof.

7 Privacy Notice

7.1 When any Personal Data is collected from an individual, they must be provided with a St. Antony's Centre Privacy Notice. The Privacy Notice provides information about what, why and how information is processed.

8 Processing, Disclosure and Sharing of Information

St. Antony's Centre processes personal data for a number of different purposes, including:

Lawful Ground for Processing of Personal Data	**Examples**
Where we have an individual's consent	Posting photographs of an individual on a website; Where an individual signs a list to confirm they want details of an event or activity; Sending individuals marketing or fundraising communication by email or SMS; Sending out newsletters or service information for which the individual has agreed previously or subscribed to

Where it is necessary for the performance of a contract to which an individual is party	Where an individual enters into an agreement with St. Antony's Centre. People signing up for a course or training
Where it is necessary for compliance with legal obligation	Passing on information to a local authority or the Charity Commission HMRC and Tax Regulation Compliance Pension Regulation Compliance Passing Gift Aid information to HMRC
Where it is necessary to protect the vital interests of an individual	Passing on information to the Police Passing on information about an individual's serious health condition to the NHS or a health professional where there is a risk of death or serious injury to that person or another individual
Where it is necessary for performance of a task in the public interest	Updating and maintaining the register of marriages
Where it is necessary for the purposes of legitimate interests pursued by St. Antony's Centre or a third party	Information, Advice and Guidance that is ongoing

Lawful Ground for Processing of Special Categories of Data	**Examples**
Where we have an individual's explicit consent	To cater for an individual's dietary or medical needs (at work, event or activity)
Where it is necessary for compliance with a legal obligation	Passing on information to a local authority or Government Agency
Where it is necessary to protect the vital interests of an individual	Passing on information to the Police Passing on information about an individual's serious health condition to the NHS or a health professional where there is a risk of death or serious injury to that person or another individual
Where it is carried out in the course of St. Antony's Centre's legitimate activities under the Charities Act	Using health related data for learners or clients Providing advice, assistance of duty of care as St. Antony's Centre
Where information has manifestly been made public	Referring to a public figure who is well known
Where we are establishing, exercising or defending legal claims	Providing information to our insurers or lawyers in connection with legal proceedings
Where the processing is for reasons of substantial public interest	Where steps are taken to prevent fraud or other dishonest activity

Where the processing is necessary for archiving historical records	Maintenance of St. Antony's Centre records, HMRC, Legal compliance or Health & Safety Data

Lawful Ground for Processing of Criminal Convictions & Offences Data	**Examples**
Where St. Antony's Centre is exercising obligations or rights which are imposed or conferred by law on it or the data subject in connection with employment, social security or social protection and the St. Antony's Centre has an appropriate policy document in place	To undertake appropriate checks on individuals prior to taking up a role For compliance with Child Protection or Vulnerable Adult Legislation and Vetting
Where it is necessary for the prevention or detection of an unlawful act	Passing on information to the Police or other investigatory body
Where St. Antony's Centre is complying with or assisting others to comply with regulatory requirements relating to unlawful acts or dishonesty	Passing on information to the Police or other legitimate investigatory body
Where it is carried out in the course of safeguarding children or other individuals at risk	Making a safeguarding disclosure
Where information is disclosed for insurance purposes	Ensuring St. Antony's Centre has appropriate insurance cover including Death in Service benefit
Where an individual has given their consent to the processing	
Where St. Antony's Centre is establishing, exercising or defending legal claims	Providing information to our insurers or lawyers in connection with legal proceedings
Where it is necessary to protect the vital interests of an individual	Passing on information to the Police or relevant body
Where it is carried out in the course of St. Antony's Centre's legitimate activities under the Charities Act	Carrying out activities and duties in line with our approved Aims and Objectives

9.1 Disclosing Personal Data

9.1.1 When receiving telephone or email enquiries, employees and volunteers should exercise caution before disclosing **any** Personal Data. The following steps should be followed:

(a) ensure the identity of the person making the enquiry is verified and check whether they are entitled to receive the requested information;

(b) require the enquirer to put their request in writing so that their identity and entitlement to receive the information can be verified if the information is particularly sensitive and/or you are not confident the person is entitled to the information;

(c) if there is any doubt, refer the request to the DPO for assistance (particularly where Special Categories of Personal Data are involved); and

(d) when providing information, ensure that Personal Data is securely packaged and sent by the most appropriate means (e.g: special delivery, courier or hand delivery) in accordance with the Data Protection Rules, the Privacy Notice and this Policy.

9.1.2 Please remember that parents and guardians are only entitled to access information about their child if the child is unable to act on their own behalf (e.g: because the child is not mature enough to understand their rights) or if the child has given their consent. If you are unsure about whether or not to provide information about a child to a parent or guardian, please speak to the DPO before providing any information. Children from 12 years upwards are generally to be taken as being capable of understanding their rights and making decision regarding their own information. However, consideration of the particular circumstances and the child's capacity must be given in each circumstance.

9.1.3 Please also remember that individuals are only entitled to obtain information **about themselves** and not any other third parties (e.g: a family member or members of staff).

10.2 Data Processors

10.2.1 St. Antony's Centre may instruct another body or organisation to process Personal Data on its behalf as a Data Processor (e.g: a payroll provider, a third-party IT provider). In such situations will share necessary information with the Data Processor, but will remain responsible for compliance with the Data Protection Rules as the Data Controller.

10.2.2 Personal Data will only be transferred to a third-party Data Processor if the DPO is satisfied that the third party has in place adequate policies and procedures to ensure compliance with the Data Protection Rules. There should also be a written contract in place between St. Antony's Centre and the Data Processor, which includes provisions to ensure that the Data Processor complies with the requirements of the Data Protection Rules and undertakings as to the inception and maintenance of appropriate measures of protection as well as insurance cover.

11.3 Third Party Requests

11.3.1 St. Antony's Centre may from time to time receive requests from third parties for access to documents containing Personal Data. St. Antony's Centre may disclose such documents to any

third party where it is legally required or permitted to do so. Such third parties may include health professionals, the Police and other law enforcement agencies, the Charity Commission, HMRC, other regulators, immigration authorities, insurers, local authorities (e.g: Trading Standards), Courts and Tribunals and organisations seeking references.

11.3.2 Anyone in receipt of any verbal or written request from any person for access to, or disclosure of, any Personal Data outside of normal St. Antony's Centre operations must immediately contact the DPO.

12.4 Transfers of Personal Data Outside of the European Economic Area ("EAA")

12.4.1 The Data Protection Rules require Data Controllers to put additional safeguards in place when transferring Personal Data outside of the EAA (e.g: ETUC or European Partners). Additionally, such transfers can only take place on a number of legal grounds. St. Antony's Centre does not store Personal Data outside of the UK. However, St. Antony's Centre may transfer Personal Data outside of the EEA where requested by the Data Subject, on the basis of the Data Subject's informed consent. This includes, but is not limited to, European Funded Programmes or Projects within the EU and its partners. The DPO may also authorize transfers where another legal ground in the Data Protection Rules is met and the request is from a legitimate authority entitled to the data.

13.5 Subject Access Requests (SARs)

13.5.1 Any Data Subject may exercise their rights as set out above. Any and all such requests should immediately be referred to the DPO.

13.5.2 To be valid, a Subject Access Request must be made in writing (including requests made via email or on social media) and provide enough information to enable St. Antony's Centre to identify the Data Subject and to comply with the request.

13.5.3 All Subject Access Requests will be dealt with by the DPO. Employees or volunteers who receive a Subject Access Request must forward it to the DPO immediately in order that such requests can be replied to within the strict deadlines set out in the Data Protection Rules (generally one month from the date of the request).

13.5.4 No fees will be charged for dealing with Subject Access Requests unless a request is considered to be manifestly unfounded, excessive or repetitive. Fees may be charged to provide additional copies of information previously provided. Where St. Antony's Centre considers a request to be manifestly unfounded, excessive or repetitive, St. Antony's Centre may lawfully refuse to respond and, if so, the DPO will inform the Data Subject of this in writing with the one-month period.

14 Fundraising and Marketing

14.1 'Direct Marketing' includes all advertising and promotional activities, including promoting the aims and deals of not-for-profit organisations / Trade Unions.

14.2 Any use of Personal Data for marketing (including fundraising) purposes must comply with the Data Protection Rules and the Privacy and Electronic Communications Regulations (EC Directive) 2003 ("PECR") (and any replacement legislation), which relate to the marketing by electronic means.

14.3 Individuals have a right to object to their Personal Data being used for electronic marketing purposes. Individuals must be informed of their right to object when their data is collected. If an objection is received, no further marketing or fundraising communications must be sent to them.

14.4 The PECR requires that St. Antony's Centre has the prior consent of recipients in certain circumstances before it sends **any** unsolicited electronic messages for the purpose of fundraising, or other marketing activities (e.g: events).

15 Monitoring and Review

15.1 This policy will be reviewed every 12 months and may be subject to change in the light of new activity, changes in legislation or other good reason.

16 Contacts

16.1 Any queries or complaints regarding Data Protection generally or this Policy specifically should be addressed to the St. Antony's Centre Data Protection Officer, who can be contacted by email kflanagan@stantonyscentre.org.uk or by telephone 0161 848 9173. If you prefer to put it in writing, the address is:

Mr K. Flanagan
St. Antony's Centre
St Antony's Centre
Eleventh Street
Trafford Park
Manchester
M17 1JF

16.2 Further advice and information can be obtained from the Information Commissioner's Office at www.ico.org.uk

17 Other Information Governance Policies

17.1 This Policy must be read in conjunction with the Policies and Guidance documents for example:

11.1.1 Privacy Notice

11.1.2 Data Retention Policy

11.1.3 Whistleblowing Policy

11.1.4 Safeguarding Policies

11.1.5 All employment related policies, e.g: disciplinary, grievance, sickness, absence, recruitment and selection

18 Glossary

"**Data Controller**" means a person, organisation or body that determines the purposes for which, and the manner in which, any Personal Data is processed. A Data Controller is responsible for complying with data protection laws including the GDPR and establishing practices and policies in line with them.

"**Data Processor**" means any person, organisation or body that processes Personal Data on behalf of an on the instruction of St. Antony's Centre. Data Processors have a duty to protect the information they process by following data protection laws.

"**Data Subject**" means a living individual about whom St. Antony's Centre processes Personal Data and who can be identified from the Personal Data. A Data Subject need to be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data and the information that St. Antony's Centre holds about them.

"**Personal Data**" means any information relating to a living individual who can be identified from that information or in conjunction with other information which is in, or is likely to come into, St. Antony's Centre's possession. Personal Data can be factual (such as a name, address or date of birth) or it can be an opinion (e.g: a performance appraisal). It can even include a simple email address. A mere mention of someone's name in a document does not necessarily constitute Personal Data, but personal details such as someone's contact details or salary (if it enabled an individual to be identified) would fall within the definition.

"**Processing**" means any activity that involves use of Personal Data. It includes obtaining, recording or holding the information or carrying out any operation or set of operations on it, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring or disclosing Personal Data to third parties.

"**Special Categories of Personal Data**" (previously called "Sensitive Personal Data") means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, condition or sexuality. It also includes genetic and biometric data. Special Categories of Personal Data can only be processed under strict conditions and such processing will usually, although not always, require the explicit consent of the Data Subject.

Signed:

K. W. Flanagan
Director

Date: 15/06/23

Publication Date:	12/12/23
Review Date:	12/12/24
Person Responsible:	Director