St John's Hospice Policies, Protocols, Guidelines & Procedures

Document Title: Confidentiality & Management of Data Policy
(Privacy, Confidentiality and Information Security Standard)

Doc Ref: SJ.HR.73

Document Type: Policy **Version:** 4

Scope: All printed and computer data

Status: Final

Authors: Sue McGraw, Chief Executive Officer
Maddy Bass, Director of Nursing & Quality
Simon Edgecombe, Medical Director
Sophy Horner, Director of Marketing, Communication & Engagement
Catherine Butterworth, Director of Income Generation
Tracey Scott, Director of Finance & Resources

Replaces: Version 3

Description of Amendments:
Privacy Notice updated: Supporter, Event Participant, Donor & Customer

Validated by: Clinical Operations & Performance Management Committee
Date: 26.07.2022

Ratified by: Chief Executive Officer/CQS Sub-committee **Date:** 09.08.22

Date of Issue: August 2022

Date of Next Revision: August 2023(Annually)

1. INTRODUCTION

St John's Hospice ("we", "our", "us", "the Hospice") is required to maintain a wide variety of records and information and is committed to ensuring that information, in whatever its context, is handled as set out by prevailing law, statute and best practice. The Hospice places significant importance on protecting personal data, yet recognises that it is imperative it shares personal information appropriately to support its service delivery functions.

This Privacy, Confidentiality and Information Security Standard ("Privacy Standard"):

- sets out how the Hospice handles the personal data of our patients, suppliers, employees, workers and other third parties.
- applies to all personal data we process regardless of the medium on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other data subject.
- applies to all Hospice personnel. You must read, understand and comply with this Privacy Standard when processing personal data on our behalf and attend training on its requirements. It sets out what we expect from you in order for the Hospice to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Please speak to the Chief Executive if you have any questions about compliance with the Privacy Standard or about data protection/information governance more generally. Any breach of this Privacy Standard may result in disciplinary action.
- together with any related policies or other Privacy Guidelines, is an internal document and cannot be shared with third parties and clients.

2. SCOPE OF THE PRIVACY STANDARD

This Privacy Standard covers the management of data, including personal data, in order to comply with current legislation, including the General Data Protection Regulation (GDPR), and best practice.

We recognise that the correct and lawful treatment of personal data will maintain confidence in the Hospice and will provide for successful operation. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The Hospice is exposed to significant fines as well as damage to our reputation if we fail to look after the personal data of our patients and other people involved in the delivery of our services as required by the GDPR.

The Chief Executive is responsible for ensuring that all Hospice personnel comply with this Privacy Standard and for implementing appropriate practices, processes, controls and training to ensure such compliance. The Chief Executive is also responsible for overseeing this Privacy Standard and for developing related policies and Privacy Guidelines as required.

Please contact the Chief Executive with any questions about the operation of this Privacy Standard or the GDPR or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the Chief Executive in the following circumstances:

a) if you are unsure of the lawful basis which you are relying on to process personal data, including the legitimate interests used by the Hospice (Section 5.1)

b) if you need to rely on Consent and/or need to capture Explicit Consent (Section 5.2)

c) if you need to draft Privacy Notices or Fair Processing Notices (Section 5.3)

d) if you are unsure about the retention period for the personal data being processed (Section 9)

e) if you are unsure about what security or other measures you need to implement to protect personal data (Section 10.1)

f) if there has been a personal data breach (Section 10.2)

g) if you need any assistance dealing with any rights invoked by a data subject (Section 12)

h) whenever you are engaging in a significant new, or change in, processing activity which is likely to require a **Data Protection Impact Assessment** (DPIA) (Section 13.4) or plan to use personal data for purposes other than what it was collected for

i) if you plan to undertake any activities involving automated processing including profiling or automated decision-making (Section 13.5)

j) if you need help complying with applicable law when carrying out direct marketing activities (Section 13.6)

k) if you need help with any contracts or other areas in relation to sharing personal data with third parties (including our vendors) (Section 13.7).

PART ONE: LEGISLATION

4. PERSONAL DATA PROTECTION PRINCIPLES

We adhere to the principles relating to processing of personal data set out in the GDPR which require personal data to be:

a) processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency)

b) collected only for specified, explicit and legitimate purposes (Purpose Limitation)

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation)

d) accurate and where necessary kept up to date (Accuracy)

e) not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation)

f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality)

g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation)

h) made available to data subjects and data subjects allowed to exercise certain rights in relation to their personal data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. LAWFULNESS, FAIRNESS AND TRANSPARENCY

5.1 Lawfulness and Fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

a) the data subject has given his or her Consent

b) the processing is necessary for the performance of a contract with the data subject to meet our legal compliance obligations;

c) to protect the data subject's vital interests (if, for example the data subject needs urgent medical assistance)

d) to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process personal data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices.

You must identify and document the legal ground being relied on for each Processing activity.

5.2 Legitimate interest

A legitimate interest is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified.

You can rely on legitimate interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object. The Hospice relies on legitimate interests for promoting its work to people on its database who have previously attended or expressed an interest in a Hospice event or campaign, or who support the work of the Hospice by volunteering. The Hospice considers this a proportionate response and, therefore, a legitimate interest.

5.3 Consent

The Hospice, as Data Controller, must only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include consent.

A data subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

Unless we can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data and for automated decision-making. Usually we will be relying on another legal basis (and not require explicit consent) to process most types of sensitive data. Where explicit consent is required, you must issue a Fair Processing Notice to the data subject to capture explicit consent.

You will need to evidence consent captured and keep records of all consents so that the Hospice can demonstrate compliance with consent requirements.

5.4 Transparency (Notifying data subjects)

The GDPR requires data controllers to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we must provide the data subject with all the information required by the GDPR including the identity of the data controller, how and why we will use, process, disclose, protect and retain that personal data through a Fair Processing Notice which must be presented when the data subject first provides the personal data.

When personal data is collected indirectly (for example, from a third party or publically available source), you must provide the data subject with all the information required by the GDPR as soon as

possible after collecting/receiving the data. You must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

6. PURPOSE LIMITATION

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the data subject of the new purposes and they have consented where necessary.

7. DATA MINIMISATION

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only process personal data when performing your job duties requires it. You cannot process personal data for any reason unrelated to your job duties.

You may only collect personal data that you require for your job duties: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Hospice's data retention guidelines.

8. ACCURACY

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

9. STORAGE LIMITATION

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Hospice will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

You will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the Hospice's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

10. SECURITY INTEGRITY AND CONFIDENTIALITY

10.1 Protecting Personal Data

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to the size of the Hospice, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. You are responsible for protecting the personal data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. You must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a) Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it

b) Integrity means those personal data are accurate and suitable for the purpose for which they are processed

c) Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

A copy of the confidentiality agreement signed by employees, workers, volunteers, students and Contractors can be found in Appendix 1.

10.2 Reporting a Personal Data Breach

The GDPR requires the Hospice to notify any personal data breach to the Information Commissioner's Office and, in certain instances, the data subject.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Chief Executive. You should preserve all evidence relating to the potential personal data breach.

11. DATA SUBJECTS' RIGHTS AND REQUESTS

Data subjects have rights when it comes to how we handle their personal data. These include rights to:

a) withdraw Consent to Processing at any time

b) receive certain information about the Hospice's processing activities

c) request access to their Personal Data that we hold

d) prevent our use of their Personal Data for direct marketing purposes

e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data

f) restrict Processing in specific circumstances

g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest

h) object to decisions based solely on Automated Processing, including profiling (ADM)

i) prevent processing that is likely to cause damage or distress to the data subject or anyone else

j) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms

k) make a complaint to the supervisory authority

l) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation).

You must immediately forward any data subject request you receive to the Chief Executive.

12. ACCOUNTABILITY

12.1 The Data Controller

The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Hospice must have adequate resources and controls in place to ensure and to document GDPR compliance including:

a) identifying an executive accountable for data privacy

b) implementing Privacy by Design when processing personal data and completing DPIAs where processing presents a high risk to rights and freedoms of data subjects

c) integrating data protection into internal documents including this Privacy Standard, any related policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices

d) regularly training Hospice personnel on the GDPR, this Privacy Standard, any related policies and/or Privacy Guidelines and data protection matters including, for example, data subject's rights, consent, legal basis, DPIA and personal data breaches. The Hospice must maintain a record of training compliance by Hospice personnel

e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

12.2 Record Keeping

The GDPR requires the Hospice to keep full and accurate records of all our data processing activities. Paper and electronic records are held by the Hospice in relation to patient and family care, personal data of personnel, volunteers and fundraising supporters.

The Hospice is required to keep and maintain accurate records reflecting our processing including records of data subjects' consents and procedures for obtaining consents. These records should include, at a minimum, the name and contact details of the Data Controller and the Chief Executive, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

12.3 Training and Audit

We are required to ensure all Hospice personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergoes similar mandatory training in accordance with the Hospice's training requirements.

You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

12.4 Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that process personal data by taking the following into account:

a) the state of the art

b) the cost of implementation

c) the nature, scope, context and purposes of Processing

d) the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

Data controllers must also conduct DPIAs in respect to high risk processing.

You should conduct a DPIA (and discuss your findings with the Chief Executive) when implementing major system or business change programs involving the processing of personal data including:

e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes)

f) automated processing including profiling and ADM

g) large scale processing of sensitive data

h) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

i) a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate

j) an assessment of the necessity and proportionality of the processing in relation to its purpose

k) an assessment of the risk to individuals

l) the risk mitigation measures in place and demonstration of compliance.

12.5 Direct Marketing

We are subject to certain rules and privacy laws when marketing to our supporters. For example, a data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing supporters known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a previous interaction with that supporter, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject's objection to direct marketing must be promptly honoured. If a supporter opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

You must comply with the Hospice's guidelines on direct marketing to supporters.

12.6 Sharing Personal Data

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the personal data we hold with another Hospice employee, agent or representative of the Hospice if the recipient has a job-related need to know the information.

You may only share the personal data we hold with third parties, such as our service providers if:

a) they have a need to know the information for the purposes of providing the contracted services

b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained

c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place

d) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

You must comply with the guidance set out in 14.6 of this Standard on sharing data with third parties.

PART TWO: BEST PRACTICE

13: ROLES & RESPONSIBILITIES

13.1 Chief Executive

The Chief Executive has overall responsibility for the management of data within the Hospice and has specific responsibility in authorising access to data. The implementation of, and compliance with, this Privacy Standard is delegated to the senior managers.

13.2 Senior Managers (Director of Nursing & Quality, Medical Director, Director of Marketing, Communications & Engagement, Director of Income Generation, Director of Finance & Resources)

The Senior Managers take responsibility for their departments in

- maintaining relevant registrations
- managing databases
- facilitating training sessions
- dealing with data access requests
- acting as the initial point of contact for any data protection issues which may arise within their Department.

13.3 Management Team

The Management Team are responsible for the day-to-day management of information and for the training of staff who use and have access to information.

13.4 Staff and Volunteers

Staff and volunteers are responsible for any records they create or use and must practice within the requirements of this Privacy Standard. Everyone who records, handles, stores or otherwise comes across information has a personal common law duty of confidence to the person the information relates to and to his or her employer.

Information should not include unreferenced abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subjective statements.

13.5 Caldicott Guardian (CG): roles and responsibilities.

The role of CG at the Hospice is held by the Director of Nursing & Quality.

This role is key in ensuring that St John's is aware of, and abides by, the highest practical standards for handling personal data, specifically patient identifiable information and patient healthcare records. The role supports the facilitation and enabling of information sharing, and advises on options for lawful and ethical data processing and processing of other information as required. The CG will work as part of a larger Information Governance (IG) function.

The CG also has a strategic role, which requires representing and championing IG requirements and issues at Board and senior management levels, and the governance framework of the Hospice. This role is particularly important in the use of IT-based patient information.

Finally, the CG should draw on a wider network of confidentiality and data protection expertise, using external advice and guidance when required.

Typical issues Hospice staff would need to refer to the CG include:

- a request from the police to access patient records
- requests from patients to delete their records
- an actual or alleged breach of confidentiality.

14. PROCEDURES AND IMPLEMENTATION

14.1 Healthcare records

Healthcare records are sensitive personal data and the requirements of clause 10.1 above must always be borne in mind in addition to the practice guidance set out in this paragraph.

Healthcare records may be held on paper and/or electronically and any member of Hospice clinical staff can contribute to the records and can write in any part of the notes as long as they are competent to have either assessed, planned, delivered or evaluated care. See the Clinical Record Keeping Standards policy (CL.02) for full guidance. Important issues communicated with patients or carers must also be recorded. Qualified professionals will be responsible for supervising the notes written by volunteers and students and whether they need a counter signature. Healthcare Assistants (HCAs) do not need their entries legally countersigned, (See Clinical Record Keeping Standard CL.02) but the RN in charge of that patient's care must be happy the HCA has the competence and capability to have records delegated to them. The HCA takes on personal accountability for the content and quality of that record.

What is written in the records must, whenever possible, be constructed with the involvement of the patient/client (as data subject) or their family carer. This is particularly pertinent to the issues of consent and the Deciding Right or Advance Care Planning record. Their feedback/comments regarding the assessment, treatment and care plan must be noted. Patients must be informed of the uses to which their personal data and any record of treatment may be put (Processed), together with any intended disclosure to outside agencies or persons as per Consent guidelines.

Hospice personnel have both a professional and a legal duty of care. Their record keeping must therefore be able to demonstrate:

- a full account of their assessment and the care that has been planned and provided
- relevant information about the condition of the patient/ client at any given time
- objectivity, not subjectivity
- the measures taken by staff to respond to needs

- evidence that staff have understood and honoured their duty of care, that all reasonable steps have been taken to care for the patient/client and that any actions or omissions have not compromised the patient's safety in any way
- a record of any arrangements that have been made for the continuing care of a patient/client
- weighing of risks and benefits
- rationales for interventions.

When not being used for patient care, all healthcare records (sensitive personal data) must be kept in a secure location, away from observation by the public, with access limited to staff working in the clinical areas.

In the community this means that no personal data should ever be left unattended, either in a locked car or in a patient's or employee's home unless kept securely. The Hospice CG recommends that they must *either* remain within the sight of the healthcare worker at all times*, or* be locked away from sight in the car boot, the latter recommended by Information Commissioners Office (ICO). Each department is responsible in ensuring this happens.

Bereavement Volunteer (BV) records (personal data) – Talking therapy may be undertaken by members of the Family Therapy Team or by qualified sessional workers or volunteers, seeing patients or relatives on behalf of Family Therapy. Records will be made in the main Healthcare Record notes for patients (sensitive personal data), but BV's may keep personal data for bereavement support, and confidential material at home. Records will be securely stored in their own home, locked away and key kept securely. This will be regularly monitored through audit. Once the client is discharged those records will be stored at the Hospice.

Any working notes or impressions of a counselling session, (that may constitute sensitive personal data) which may serve as an aide memoir to subsequent sessions for example, will be retained for 12 months before being destroyed. During the period in which such records are kept, they will be subject to client access under the GDPR provisions and will be available within the Family Therapy filing system.

Research, teaching and supervision - patient/client records may be used for research, teaching purposes, audit and clinical supervision subject to compliance with the GDPR. The principles of access and confidentiality are paramount and the right of the data subject (usually the patient) to refuse access to their sensitive personal data must be respected. The local research ethics committee must approve the use of patient/client records in research. It is best practice to anonymise/pseudonymise these as much as possible prior to them being used for such purposes.

14.2 Photographs, videos and CCTV

Consent is always obtained from individuals who have been photographed or recorded for Hospice communication purposes via the publicity consent form unless it is a public event outside the Hospice, e.g. a fundraising walk. The consent form must contain a clear Privacy Statement stating

what the personal data information may be used for (processed) and asks the data subject to state if they wish the image or broadcast to be used for one occasion only or in perpetuity.

The Hospice maintains CCTV coverage of the premises for the purposes of crime prevention and the safety of staff, patients and visitors following the code of practice laid out by the ICO and under the rules of the Data Protection Act 2018. Information on how we manage our CCTV operation is contained in the Hospice's CCTV Policy.

Photographs/video/audio recordings, and consent forms, are stored by the fundraising and marketing staff, which only is accessible by Hospice personnel with appropriate authority.

On the advice of the ICO, all archived photographs (i.e. pre May 2008) are used only when no individual data subject is identifiable. For example, as a group shot or with a general image that doesn't carry a caption.

See Appendix 2 for the consent form.

14.3 Personnel and Volunteer Personal Data

Personnel and personal records contain personal data, and may contain sensitive personal data. Personnel records are defined as information about employees, volunteers, contractors or temps, created or received in the course of business, and captured in a readable form in any medium, providing evidence of the functions, activities and transactions of those people. These may be held by the HR department or by the person's line manager.

14.4 Fundraising data

Fundraising records contain personal data. Fundraising records are defined as information about people created or received in the course of fundraising and captured in a readable form in any medium, providing evidence of the functions, activities and transactions of those people. These will be held in the Donorflex system. The Director of Income Generation is responsible for ensuring the Fundraising and Supporter Care teams are aware of their responsibilities in this area. Fundraisers handle data in accordance with the latest Fundraising Regulatory Standards.

Appropriate Privacy Notices are included in the forms on which personal data of fundraisers or other supporters are collected.

14.5 Access to health records (sensitive personal data)

Formal and Informal access to health records – access to health records has always occurred on a voluntary and informal basis between clinician and patient (the data subject). Whenever possible, access should be given in this way whilst a patient is undergoing treatment or care. It only applies to particular episodes of care to which the applicant actually refers and is not an opportunity for the applicant to peruse the complete medical notes.

14.6 Sharing Personal Data

The requirements of the GDPR set out in clause 12.6 must be complied with**.** In some circumstances, confidentiality is not absolute and it might be essential that it be breached. This may be appropriate where it becomes necessary to protect an individual from harm such as in a child protection case, protection of vulnerable adults, or where personal information is required for a serious crime investigation. Disclosure is sometimes required without consent: for example, public health legislation stipulates that designated St John's Hospice staff must notify the relevant authority where a person is suspected of contracting a notifiable disease.

Where information would be disclosed without or against the consent of the individual, for example because the information is required under a court order/statute or there is an over-riding public interest for doing so, the decision to release information should be referred to the CG, who will make a judgement on a case-by-case basis. It may be appropriate for legal or specialist advice to be sought if information is to be disclosed without the individual's consent.

Each case should be judged on its merits whether a disclosure without consent is justified. Decisions must be made by those with delegated powers within St John's Hospice.

Information, which has been aggregated or anonymised, can generally be shared for justified purposes. Care should be taken to ensure that individuals cannot be identified from this type of information, as it is frequently possible to identify individuals from limited data. If individuals can be identified by the data it is personal data and the GDPR will apply. In all cases only the minimum identifiable information necessary to satisfy the purpose should be made available.

Where St John's Hospice receives a request for personal information from organisations, such as the Police or regulatory bodies, certain information can be released, e.g.

- The Police have produced a court order
- The information is required under the Road Traffic Act
- Requirement to refer to a professional regulatory body e.g. Fitness to practise, NMC/GMC

Where there is no legal compulsion to disclose and the consent of the individual has not been obtained to release their information, the Hospice can consider whether to disclose but must justify any decision to do so.

14.7 Controlled Drugs

The Hospice is part of an Information Sharing Protocol with the Local Intelligence Network (LIN) through the Accountable Officer. This facilitates the sharing of concerns, suspicions and incidents in relation to Controlled Drugs and can allow for advice and support. The Accountable Officer for the Hospice is responsible for the sharing of any relevant information. This position is held by the Director of Nursing & Quality.

14.8 Information technology

The Hospice is committed to providing information resources to help staff work in an efficient manner. Staff are expected to use these resources responsibly and not to abuse the trust placed on them. Staff must conduct themselves honestly and respect copyright, licensing, property rights and the privacy of others. Guidance on appropriate usage is found in the Professional Behaviours at St John's policy (HR.41) and in the Disciplinary Procedure (HR.13).

Electronic communications facilities include:

- Website
- Electronic mail
- Social networking sites, e.g. Facebook, Twitter, which may be used for marketing purposes
- Internet usage
- Use of PCs, Laptops, PDAs, smart phones
- Audio visual devices, e.g. video camera.
- Telephone equipment including mobile phones, dictaphones and voicemail
- Digital cameras including mobile phone cameras
- Any type of mobile data storage device (CDs, data sticks etc.)
- Personal communication facilities e.g. working from home on own devices using office 365.

The Hospice website will ensure that:

- Users must be able to opt out of any disclosure
- Users must be advised who will be using the information and who it may be disclosed to
- Users must be advised of Cookie usage
- Privacy Notices are available (See appendix 3).

The principles for electronic record keeping are the same as for paper records. In addition, when using electronic documentation, it is advisable to have the correct procedures in place to ensure:

- Physical security/equipment security
- Access control (at different levels, if necessary)
- User password management for all IT systems: this should include changing of passwords regularly as best practice
- Computer virus control
- Data back-up
- Computer network management

- Data and software exchange
- Validation
- Adequate training for all users.

Where both computer and paper systems are maintained, the information held must be consistent.

14.9 Use of the Internet

Hospice Personnel must not:

a) Access illegal, pornographic, obscene, abusive (racially or sexual) internet sites from work

b) Use the Internet for private commercial, political or other non work related purposes, or for making personal profit

c) Use the Internet to download software or other programs without seeking prior approval of the Hospice's Chief Executive or UHMBFT. This is most important because of the potential risk of downloading malicious programs.

d) Use the Internet at work for personal internet "chatting", messaging or for playing computer games.

e) Subscribe to any bulletin boards, newsgroups or any other internet service of any kind without prior discussion with their line manager unless relevant to the work role, e.g. Hospice UK bulletin.

f) Download, copy or transmit to third parties the works of others without their permission as this may infringe copyright.

g) Use public social networking sites to discuss work related issues unless promoting fundraising events on local and appropriate sites, e.g. Cumbria Crack.

14.10 Mobile Computers

Handheld personal digital assistants (PDA's), Smartphones and Laptops offer portability, access to data when away from the desktop PC and are a useful tool for business use. Due to their portability certain security risks arise namely:

- easy to lose or damage
- they can be easily stolen
- they have limited security features
- they can hold a great deal of information that could be sensitive or confidential in nature
- they have the ability to transmit viruses to any host PC that they are connected to.

Therefore, staff should:

- ensure that Laptops, Smartphones, Tablets and PDAs are password protected

- access sensitive or confidential information remotely and not save it onto the computer's local drive
- ensure that the laptop is stored securely when not in use.

14.11 Retention, Destruction and Disposal

The Hospice has a separate policy for the retention, destruction and disposal of records containing personal data. See policy HR.74.

15. CHANGES TO THIS PRIVACY STANDARD

The Hospice reserves the right to change this Privacy Standard at any time.

You will be informed of the change and the updated version of the Privacy Standard made available to you.

16: APPENDICES

Appendix 1 - Confidentiality Agreement

Appendix 2 – Public Consent Form

Appendix 3 – Privacy Notices

- Patients, Families and Clients
- Recruitment of Employees or Workers
- Employees, Workers and Contractors (UK)
- Recruitment of Volunteers
- Volunteers
- Recruitment of Contractors
- Supporter, Event Participant, Donor and Customer

Appendix 1

Confidentiality Agreement

PROTECTING AND USING INFORMATION

It is the responsibility of all individuals; employees, workers, volunteers, students and contractors of St John's Hospice & St John's Hospice Shops Ltd (*herein after called 'the Hospice'*) to be aware of the legislation in place to protect personal information (confidentiality).

Personal information is held by the Hospice which may relate to patients and other people who use our services, as well as employees, workers, volunteers, contractors, supporters and customers. Legislation covers personal information held or processed in the following formats: computer held records, email communications, computer printouts, CCTV, fax, telephone and any written information used (personal files, payroll records etc.). Misuse of personal information may lead to prosecution of an individual under the Data Protection Act 2018.

There are eight principles of data protection. St. John's Hospice abides by the Data Protection Act 2018 & General Data Protection Regulations 2018. The Act dictates that information should only be disclosed on a need to know basis.

- ✓ Personal data shall be processed fairly and lawfully.
- ✓ Personal data shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose.
- ✓ Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.
- ✓ Personal data shall be accurate and where necessary, kept up to date.
- ✓ Personal data processed for any purpose shall not be kept longer than necessary.
- ✓ Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act
- ✓ Appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- ✓ Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country ensures an adequate level of protection of the rights of data subjects in relation to the processing of personal data.

The Copyright Designs and Patents Act 1988 This Act makes the use of unlicensed (pirated) software a criminal offence, which could lead to fines or imprisonment.

The Computer Misuse Act 1990 This Act makes it a criminal offence to access any part of a computer system programs and/or data that you are not set up to access, e.g. access a record of someone you may know; share someone's password or access a system which is not for the St. John's Hospice's purposes. Each system/network has an individual user ID and password. This should remain confidential to those authorised to access those records.

Confidentiality

All information you come in contact with during the course of your work must be deemed to be confidential. This will apply to records relating to patients and their friends and relatives, applicants, staff, volunteers, contractors, community members, supporters and other medical personnel and may also include business sensitive information.

Under no circumstances should any of this information be divulged or passed on to any unauthorised persons by you whilst you are carrying out your role at the Hospice or after your relationship with the Hospice ends. A breach of confidentiality may lead to disciplinary or legal action.

If you have any questions relating to confidentiality of information or wish to raise a concern please speak to Sue McGraw, CEO.

I confirm that I have read the above statement, understand my responsibilities and agree to abide by the Hospice's policies and procedures in relation to personal data.

Name: _____

Job or Role: _____

Signature: _____

Date: _____

Appendix 2

PUBLICITY CONSENT FORM

Please print all information in CAPITALS.

Name (of person in photo / video / quoted etc): ***Required***
Why is the photo / video / quote etc being taken?
Address: **Postcode:**
Name of carer / next of kin / guardian: (if signing on behalf of a child under 18 years of age or for a patient who lacks capacity) **Relationship to the above:**
Address: **Postcode**
Contact phone number: **Email address:**

I hereby give permission for St John's Hospice to use my: (please delete as appropriate)

- image / photograph
- voice recording
- audio/visual recording (filming)
- interview
- quote, comments and feedback for third party purposes e.g. press
- story

For promotional purposes:

☐ Used on one occasion

☐ Used for perpetuity

I understand that this may include, but is not limited to, use on the St John's Hospice website, third party websites that promote the Hospice's services or fundraising events, local and national media (print, online, broadcast), social networking websites, and printed and digital literature.

I understand that I may withdraw my consent at any time by contacting the St John's Hospice Communications team on 01524 382538.

St John's Hospice may actively use my information for publicity purposes for up to three years. I also understand, however, that if content (e.g. photograph) is in use (e.g. in a printed leaflet), it may continue to be used for a period of time after this consent period has ended until the material is reviewed. It could potentially be used in the future - after the three year consent period has ended – specifically in relation to retrospective materials about key historic milestones and events.

Date: ***Required***

Signature: ***Required***

Appendix 3

Privacy notice – Patients, families and clients

WHAT IS THE PURPOSE OF THIS DOCUMENT?

St John's Hospice is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you and your family during and after your care with us, in accordance with the General Data Protection Regulation (GDPR).

It applies to all patients, families and clients who use our services.

St John's Hospice is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former patients, families and clients. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed

(anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection, such as information about a person’s health or sexual orientation.

We will collect, store, and use the following categories of personal information about you:

Patient’s Personal Information Retained

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Date of birth
- Ethnicity
- Gender
- Religion
- NHS number
- Marital status and dependants
- Emergency contact (first contact) information
- Employment records (including job titles, work history) if patient happy to share, and if disease may be industrial caused
- Complaints and grievance information (but this is not stored as part of your clinical record)
- CCTV footage if you are cared for on-site
- Photographs of wounds or, with explicit consent, other photos such as for fundraising or for raising the profile of SJH work
- DNACPR documentation, recording whether agreed with resuscitation decision
- Preferred Place of Care and Preferred Place of Death
- Home key safe details (usually as an alert on EMIS records)
- Safeguarding risks (usually as an alert on EMIS records)
- Informing the authorities of notifiable diseases you may have at the time
- Any details discussed with the coroner
- Additional support needs, such as mental health, sensory impairment and mobility requirements
- Which services are accessed

- Appointment attendance details, schedule and ongoing plan
- Inter-practice communications pertaining to the circumstances of your care

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions
- Information about your health, including any medical condition, health and sickness records, including medical condition, current and historical diagnoses, health and sickness records, previous encounters with other GPs, consultants, community nurses and medical institution staff, medical test results
- Detailed records of medical encounters between yourself and healthcare professionals
- Medications currently and historically taken
- Record of capacity to give consent (Mental Capacity Act 2005)
- Allergies and intolerances
- Safeguarding risks pertaining to mental health or criminal convictions

Use of this personal information

- Making a decision about your current and future healthcare such as a referral, transfer, change of medication, equipment order
- Informing ongoing healthcare practice to meet your specific needs
- Reviewing your condition prior to an encounter to ensure continuity of care
- Informing other clinicians and services involved in your care about your condition, treatment and requirements
- To contact yourself, or your approved contacts if you lack capacity for these discussions, about current and future care objectives or to inform about a schedule alteration concerning these objectives
- To conduct data analytics studies and research to review and improve ongoing hospice and palliative care standards
- Gathering evidence for possible grievance, disciplinary or complaint proceedings
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents on site (RIDDOR)

- Ascertaining the most appropriate services to be offered
- Complying with health and safety obligations, including access and nutritional needs
- Equal opportunities monitoring and equality of access improvements
- To book ambulance or volunteer transport for movement between your home and the hospice site

Next of Kin / First Contacts / Carers Personal Information Retained

- Personal contact details such as name, title, addresses, telephone numbers and personal email addresses of the patient states you are one of their main contacts
- Marital status and dependents
- Complaints and grievance information, but only if you are involved in the process and this would be kept separate to your clinical records
- CCTV footage if on site
- Additional support needs such as mental health, sensory impairment and mobility requirements
- Which services are accessed (bereavement, spiritual care) and records of activity
- Communications with health care professionals and administrative support staff

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Record of capacity to give consent (Mental Capacity Act 2005) especially if you, the patient, lacks capacity and the hospice is speaking to 'patient representatives' to make a best interests decision
- Allergies and intolerances
- Safeguarding risks pertaining to mental health or criminal convictions

Use of this personal information

- To contact yourself or your approved contacts about current and future care objectives or to inform about a schedule alteration concerning these objectives if you, the patient, lacks capacity and your next of kin is the first contact or have an LPA WD
- To alert them to changes in the patient's condition, such as deterioration or death
- To complete and forward consented referrals to support services
- Conducting service performance reviews, managing performance and determining performance

requirements

- Gathering evidence for possible grievance, disciplinary or complaint proceedings but would be kept separate from patient's clinical records and their own clinical/bereavement record
- Dealing with legal disputes involving them or other employees, worker and contractors, including accidents on site
- Ascertaining the most appropriate services to be offered
- Complying with health and safety obligations
- Equal opportunities monitoring and equity of access improvements
- Informing the authorities of notifiable diseases they may have at the time

Bereavement/Spiritual Care Clients Personal Information Retained

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- Date of birth
- Ethnicity
- Gender
- Religion
- Marital status and dependents
- Next of kin and emergency contact information
- CCTV footage if on site
- Photographs with explicit consent such as for fundraising or raising the profile of SJH work
- Records of contacts with support volunteers and groups
- Personal details of the associated patient including name, diagnosis, date and place of death and address

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about their race or ethnicity, religious beliefs, sexual orientation and political opinions (only if the client chooses to share this with us and we feel it would help us support them)
- Information about their health, including any medical condition, health and sickness records

Use of this personal information

- Inviting them to participate in any groups or events relating to spiritual or bereavement support
- Fowarding remembrance and condolence communications, including anniversary cards
- To provide context to bereavement volunteers in order to inform the nature of the care provided to them and best meet their individual needs
- Gathering evidence for possible grievance, disciplinary or complaints proceedings but would be kept separate from patient's clinical records and their own clinical/bereavement record
- Inviting them to participate in service feedback surveys and groups
- Complying with health and safety obligations
- Equal opportunities monitoring and equity of access improvements
- Informing the authorities of notifiable diseases they may have at the time

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about patients, families and clients through the admission and referral process, either directly from you or from existing medical records which you have consented to us having access to

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where processing is necessary for medical diagnosis, provision of health or social care or treatment (GDPR 9(2)h)
- Where we need to keep you safe, e.g. when there is a safe guarding risk to you
- Where we need to comply with a legal obligation
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the care

we would like to or we may be prevented from complying with our legal obligations, such as making sure you have the ability to make important decisions, or to be cared for in the best place.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

DATA SHARING

We will share your clinical records with other health and social care staff to ensure you have safe and effective care at all times, both within the hospice building and in the community.

We require third parties to respect the security of your data and to treat it in accordance with the law.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer your care safely or where we have another legitimate interest in doing so. We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to CQC, or local safeguarding teams.

Which third-party service providers process my personal information?

"Third parties" includes other service providers involved in your care. This can include NHS services such as hospital or community teams, social care services, care homes, GPs, district nursing teams, etc. – it very much depends on which services can help you most.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We only permit third-party service providers to process your personal data for specified purposes and in accordance with our instructions. They will also require your consent to access your health records.

Transferring information outside the EU

We do not envisage that your personal information will be transferred outside the EU, however we will notify you in writing if this position changes.

DATA SECURITY

We have put in place measures to protect the security of your information. Details of these

measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, volunteers and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Director of Nursing and Quality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. For health care records this is usually 8 years from our final contact with you. Retention depends on the sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you

have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Director of Nursing and Quality, in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Volunteer Coordinator. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

DATA PROTECTION OFFICER

If you have any questions about this privacy notice or how we handle your personal information, please contact the Director of Nursing and Quality. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the Director of Nursing and Quality.

Privacy notice – Recruitment of Employees or Workers

WHAT IS THE PURPOSE OF THIS DOCUMENT?

St John's Hospice is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. You are being sent a copy of this privacy notice because you are applying for work with us (whether as an employee or worker). It makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under the General Data Protection Regulation (*(EU) 2016/679*) (GDPR).

DATA PROTECTION PRINCIPLES

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

In connection with your application for work with us, we will collect, store, and use the following categories of personal information about you:

- The information you have provided on our application form, including name, title, address, telephone number, personal email address, gender, employment history, qualifications.
- The supporting information you may have provided to us in your curriculum vitae and covering letter or email.
- Any information you provide to us during an interview.
- Any other information you provide to us as part of the application process, for example presentations or practical test results.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about candidates from the following sources:

- You, the candidate.
- Disclosure and Barring Service in respect of criminal convictions (if the position is eligible for a DBS check).
- Your named referees, from whom we collect the following categories of data: Attendance, Disciplinary, Suitability.

HOW WE WILL USE INFORMATION ABOUT YOU

We will use the personal information we collect about you to:

- Assess your skills, qualifications, and suitability for the position you have applied for.
- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- Comply with legal or regulatory requirements.

It is in our legitimate interests to process the information you have provided to enable us to decide whether to offer you employment in the position you have applied for.

We also need to process your personal information to decide whether to enter into a contract of employment with you.

Having received your application form (and supporting CV if provided) we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to call you for an interview, we will use the information you provide to us at the interview to decide whether to offer you the position. If we decide to offer you the position, we will then take up references, carry out a criminal record check, establish that you have the right to work in the UK, and require you to be assessed by our occupational health provider as fit to work. You will also be required to provide original documentation to prove you hold the qualification(s), if any, that are required for the position, including Full UK Driving Licence, where relevant. If you are offered a position which requires you to be registered with a governing body, i.e. GMC or NMC we will check

your registration online. We will carry out all these checks before confirming your appointment.

If you fail to provide personal information

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require a criminal record check or references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

We will use your particularly sensitive personal information in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We envisage that we will process information about criminal convictions.

We will collect information about your criminal convictions history if we would like to offer you employment (conditional on checks and any other conditions, such as references, being satisfactory) in a role which may bring you into contact with vulnerable adults or young people. We are entitled to carry out a criminal lrecords check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. In particular:

- We are legally required by Care Quality Commission to carry out criminal record checks for those carrying out regulated activities as defined by the Safeguarding Vulnerable Groups Act 2006 as amended by the Protection of Freedoms Act 2012.
- If the role for which you are applying is one which is listed on the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (*SI 1975/1023*) and is also specified in the Police Act 1997 (Criminal Records) Regulations (*SI 2002/233*)] so is eligible for a standard or enhanced check from the Disclosure and Barring Service.

We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.

AUTOMATED DECISION-MAKING

We do not use recruitment software which makes autonomous shortlisting decisions.

DATA SHARING

Why might you share my personal information with third parties?

We will only share your personal information with the following third parties for the purposes of processing your application: Sage Occupational Health; Disclosure & Barring Service. All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

DATA SECURITY

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Head of Human Resources.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

How long will you use my information for?

We will retain your personal information for a period of 6 months after we have communicated to you our decision about whether to appoint you to the position you have applied for. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with our data retention policy.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised

your right to object to processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Head of Human Resources in writing.

RIGHT TO WITHDRAW CONSENT

You have the right to withdraw your consent for us to process your information at any time during the recruitment process. Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our retention policy, we will dispose of your personal data securely. To withdraw your consent, please contact the Head of Human Resources.

DATA PROTECTION

If you have any questions about this privacy notice or how we handle your personal information, please contact the Chief Executive. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Privacy notice for employees, workers and contractors (UK)

WHAT IS THE PURPOSE OF THIS DOCUMENT?

St John's Hospice is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

It applies to all employees, workers and contractors.

St John's Hospice is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that

person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection, such as information about a person's health or sexual orientation.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth
- Gender
- Marital status and dependants
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information
- Start date and, if different, the date of your continuous employment
- Leaving date and your reason for leaving
- Location of employment or workplace
- Copy of driving licence
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Employment records (including job titles, work history, working hours, holidays, training records, qualifications, professional memberships and relevant indemnity insurances)
- Compensation history
- Performance information
- Disciplinary and grievance information
- CCTV footage and other information obtained through electronic means such as door entry fob records
- Information about your use of our information and communications systems
- Photographs, e.g. for staff newsletters, ward board photos, etc.

- Results of HMRC employment status check, details of your interest in and connection with the intermediary through which your services are supplied.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Information about your health, including any medical condition, health and sickness records, including:
    - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
    - where you leave employment and the reason for leaving is related to your health, information about that condition needed for pensions and permanent health insurance purposes.
- Information about criminal convictions and offences

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about employees and workers through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, Disclosure & Barring Service and Occupational Health provider.

We may also collect personal information from the trustees or managers of pension arrangements operated by a group company on our behalf.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest.

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with employment.
- Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our occupational pension scheme].

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance.
- If you apply for an ill-health pension under a pension arrangement operated by a group company, we will use information about your physical or mental health in reaching a decision about your entitlement.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our Disclosure & Barring Service Policy and our Privacy Confidentiality & Information Security Standard Policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process and every three years thereafter or we may

be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

- To assess if you are suitable to work with vulnerable adults and/or children and young people.

We are allowed to use your personal information in this way to carry out our obligations under the Safeguarding Vulnerable Adults Act 2006 as amended by the Protection of Freedoms Act 2012. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

AUTOMATED DECISION-MAKING

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

DATA SHARING

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: pension administration, occupational health services, benefits provision and administration, IT services.

We will share personal data regarding your participation in any pension arrangement operated by a group company with the trustees or scheme managers of the arrangement in connection with the administration of the arrangements.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them

to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to HMRC.

Transferring information outside the EU

We do not envisage that your personal information will be transferred outside the EU, however we will notify you in writing if this position changes.

DATA SECURITY

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Head of Human Resources.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting

requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available on the shared drive. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to

another party, please contact the Head of Human Resources in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Head of Human Resources. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

DATA PROTECTION

If you have any questions about this privacy notice or how we handle your personal information, please contact the CEO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact the CEO.

Privacy notice – Recruitment of Volunteers

WHAT IS THE PURPOSE OF THIS DOCUMENT?

St John's Hospice is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. You are being given a copy of this privacy notice because you are applying for volunteer work with us. It makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under the General Data Protection Regulation (*(EU) 2016/679*) (GDPR).

DATA PROTECTION PRINCIPLES

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

In connection with your application for work with us, we will collect, store, and use the following categories of personal information about you:

- The information you have provided on our application form, including name, title, address, telephone number, personal email address, gender, date of birth, employment history, qualifications.
- Any information you provide to us during an interview.
- Any other information you provide to us as part of the application process.
- Photographs for identification purpose.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about candidates from the following sources:

- You, the applicant.
- Disclosure and Barring Service in respect of criminal convictions (if the position is eligible for a DBS check).
- Your named referees, from whom we collect the following categories of data: Reliability & Punctuality; Trustworthiness and Teamwork

HOW WE WILL USE INFORMATION ABOUT YOU

We will use the personal information we collect about you to:

- Assess your skills, qualifications, and suitability for the volunteer position you have applied for.
- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our recruitment processes.
- Comply with legal or regulatory requirements.

It is in our legitimate interests to process the information you have provided to enable us to decide whether to offer you a volunteer position with either St John's Hospice or St John's Hospice Shops Ltd.

Having received your application form (and supporting CV if provided) we will then process that information to invite you for an interview. We will use the information you provide to us at the interview to decide whether to offer you a voluntary position. If we decide to offer you a position, we will then take up references, carry out a criminal record check, establish that you have the right to work in the UK. You may also be required to provide original documentation to prove you hold the qualification(s), if any, that are required for specific volunteer postions, including Full UK Driving Licence. If you are offered a volunteer position which requires you to be registered with a governing body, i.e. Federation of Holistic Therapists we will check your registration online. We will carry out all these checks before confirming your appointment.

If you fail to provide personal information

If you fail to provide information when requested, which is necessary for us to consider your application we will not be able to process your application successfully. For example, if we require a criminal record check or references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

We will use your particularly sensitive personal information in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during the interview.
- We will use information about your race or national or ethnic origin, religious, philosophical or

moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We envisage that we will process information about criminal convictions.

We will collect information about your criminal convictions history if we would like to offer you a volunteer position (conditional on checks and any other conditions, such as references, being satisfactory) in a role which may bring you into contact with vulnerable adults or young people. We are entitled to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. In particular:

- We are legally required by Care Quality Commission to carry out criminal record checks for those carrying out regulated activities as defined by the Safeguarding Vulnerable Groups Act 2006 as amended by the Protection of Freedoms Act 2012.
- If the role for which you are applying is one which is listed on the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (*SI 1975/1023*) and is also specified in the Police Act 1997 (Criminal Records) Regulations (*SI 2002/233*)] so is eligible for a standard or enhanced check from the Disclosure and Barring Service.

We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.

AUTOMATED DECISION-MAKING

We do not use recruitment software which makes autonomous shortlisting decisions.

DATA SHARING

Why might you share my personal information with third parties?

We will only share your personal information with the following third parties for the purposes of processing your application: Disclosure & Barring Service. All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

DATA SECURITY

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Head of Human Resources.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

How long will you use my information for?

We will retain your personal information for a period of 6 months after we have communicated to you our decision about whether to offer you a voluntary position at St John's Hospice or St John's Hospice Shops Ltd. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with our data retention policy.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Volunteer Coordinator in writing.

RIGHT TO WITHDRAW CONSENT

You have the right to withdraw your consent for us to process your information at any time during the recruitment process. Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our retention policy, we will dispose of your personal data securely. To withdraw your consent, please contact the Volunteer Coordinator.

DATA PROTECTION

If you have any questions about this privacy notice or how we handle your personal information, please contact the Chief Executive. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Privacy notice - Volunteers

WHAT IS THE PURPOSE OF THIS DOCUMENT?

St John's Hospice is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your volunteering relationship with us, in accordance with the General Data Protection Regulation (GDPR).

It applies to all volunteers.

St John's Hospice is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former volunteers. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection, such as information about a person's health or sexual orientation.

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth
- Gender
- Marital status and dependants
- Next of kin and emergency contact information
- National Insurance number
- Start date
- Leaving date and your reason for leaving
- Location of employment or workplace
- Copy of driving licence
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Volunteer records (including volunteer roles, volunteering history, volunteer hours, holidays, training records and professional memberships)
- Performance information
- CCTV footage and other information obtained through electronic means such as door entry fob records
- Information about your use of our information and communications systems
- Photographs, e.g. for badges, identification and promotion of 'Volunteers Week' with your permission.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions
- Information about your health, including any medical condition, health and sickness records, including:
    - details of any absences (other than holidays) from your volunteering role
- Information about criminal convictions and offences

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about volunteers through the application and recruitment process, either directly from candidates or sometimes from a volunteer agency or background check provider. We may sometimes collect additional information from third parties including former employers and Disclosure & Barring Service.

We will collect additional personal information in the course of volunteer-related activities throughout the period of you volunteering for us.

LEGITIMATE INTERESTS

A legitimate interest is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified.

We can rely on legitimate interests for marketing activities if we can show that how we use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object. The Hospice relies on legitimate interests for promoting its work to people on its database who have previously attended or expressed an interest in a Hospice event or who support the work of the Hospice by Volunteering. The Hospice considers this a proportionate response and, therefore, a legitimate interest. However you can opt out of this anytime by contacting the Supporter Care team at the Hospice.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the volunteer agreement we have entered into with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the agreement we have entered into with you, or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with volunteering.
- Where it is needed in the public interest, such as for equal opportunities monitoring.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to volunteer, to provide appropriate workplace adjustments, to monitor and manage sickness absence.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our Disclosure & Barring Service Policy and our Privacy Confidentiality & Information Security Standard Policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process and every three years thereafter or we may be notified of such information directly by you in the course of you volunteering for us. We will use information about criminal convictions and offences in the following ways:

- To assess if you are suitable to volunteer with vulnerable adults and/or children and young people.

We are allowed to use your personal information in this way to carry out our obligations under the Safeguarding Vulnerable Adults Act 2006 as amended by the Protection of Freedoms Act 2012. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

AUTOMATED DECISION-MAKING

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

DATA SHARING

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the volunteer relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: IT services.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data.

What about other third parties?

We may share your personal information with other third parties, for example in the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal data with the other parties if and to the extent required under the terms of the transaction.

We may also need to share your personal information with a regulator or to otherwise comply with the law.

Transferring information outside the EU

We do not envisage that your personal information will be transferred outside the EU, however we will notify you in writing if this position changes.

DATA SECURITY

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Volunteer Coordinator.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available on the shared drive. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be

associated with you, in which case we may use such information without further notice to you. Once you are no longer a volunteer of the company we will retain and securely destroy your personal information in accordance with our data retention policy.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your volunteering relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the HR Coordinator in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person

who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Volunteer Coordinator. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

DATA PROTECTION

If you have any questions about this privacy notice or how we handle your personal information, please contact the CEO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Privacy notice – Recruitment of Contractors

WHAT IS THE PURPOSE OF THIS DOCUMENT?

St John's Hospice is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. You are being sent a copy of this privacy notice because you are applying for work with us as a contractor. It makes you aware of how and why your personal data will be used, namely for the purposes of the procurement exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under the General Data Protection Regulation (*(EU) 2016/679*) (GDPR).

DATA PROTECTION PRINCIPLES

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

In connection with your application to provide services us, we will collect, store, and use the following categories of personal information about you:

- The information you have provided on our Contractor Compliance and Competence Questionnaire, including your name, the name of your business or the business you work for, your position in the business, the address of the business, telephone number, email address, details to support your competence to deliver the service and details of your Public Liability and Employer Liability insurance provider.
- The supporting information you may have provided to us in your covering letter or email.
- Any information you provide to us during a meeting relating to the procurement of services.
- Any other information you provide to us as part of the procurement process, for example presentations or demonstrations.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about contractors from the following sources:

- You, the candidate.
- Your named referees, from whom we collect the following categories of data: Competence and Suitability.
- Health & Safety Executive in respect of health and safety breaches.
- Disclosure and Barring Service in respect of criminal convictions (if the position is eligible for a DBS check).

HOW WE WILL USE INFORMATION ABOUT YOU

We will use the personal information we collect about you to:

- Assess your skills, qualifications, and suitability for the contract you have applied for.
- Carry out background and reference checks, where applicable.
- Communicate with you about the procurement process.
- Keep records related to our hiring processes.
- Comply with legal or regulatory requirements.

It is in our legitimate interests to process the information you have provided to enable us to decide whether to enter into a contract for services with you.

Having received your Contractor Compliance and Competence Questionnaire we will then process that information to decide whether you meet the basic requirements to be shortlisted for the contract. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to call you for an interview, we will use the information you provide to us at the interview to decide whether to offer you a contract. If we decide to offer you a contract, we will then take up references, carry out a prosecution history check with the Health & Safety Executive and establish that you have the right to work in the UK. In some instances we may undertake a criminal records check. You will also be required to provide original documentation to prove you hold the qualification(s), if any, that are required for the position, for example Gas Safety Mark. If you are offered a position which requires you to be registered with a governing body, i.e. GMC or NMC we will check your registration online. You will also be required to provide original documentation to prove you hold Public Liability Insurance and, where relevant, Employer's Liability Insurance. We will carry out all these checks before confirming your appointment.

If you fail to provide personal information

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or indemnity insurance), we will not be able to process your application successfully. For example, if we require a criminal record check or references for this contract and you fail to provide us with relevant details, we will not be able to take your application further.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

We will use your particularly sensitive personal information in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We envisage that in certain circumstance we will process information about criminal convictions. If we need to do this we will advise you at the start of the procurement procedure.

We will collect information about your criminal convictions history if we would like to offer you a contract for services (conditional on checks and any other conditions, such as references, being satisfactory) in a role which may bring you into contact with vulnerable adults or young people. We are entitled to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. In particular:

- We are legally required by Care Quality Commission to carry out criminal record checks for those carrying out regulated activities as defined by the Safeguarding Vulnerable Groups Act 2006 as amended by the Protection of Freedoms Act 2012.
- If the role for which you are applying is one which is listed on the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (*SI 1975/1023*) and is also specified in the Police Act 1997 (Criminal Records) Regulations (*SI 2002/233*)] so is eligible for a standard or enhanced check from the Disclosure and Barring Service.

We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data.

AUTOMATED DECISION-MAKING

We do not use recruitment software which makes autonomous shortlisting decisions.

DATA SHARING

Why might you share my personal information with third parties?

We will only share your personal information with the following third parties for the purposes of processing your application: Disclosure & Barring Service, Health & Safety Executive. All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

DATA SECURITY

We have put in place appropriate security measures to prevent your personal information from

being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Head of Facilities.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

How long will you use my information for?

We will retain your personal information for a period of 6 months after we have communicated to you our decision about whether to appoint you as a contractor. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the procurement exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with our data retention policy.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Head of Facilities in writing.

RIGHT TO WITHDRAW CONSENT

You have the right to withdraw your consent for us to process your information at any time during the recruitment process. Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our retention policy, we will dispose of your personal data securely. To withdraw your consent, please contact the Head of Facilities.

DATA PROTECTION

If you have any questions about this privacy notice or how we handle your personal information, please contact the Chief Executive. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Privacy notice – Supporter, Event Participant, Donor and Customer

WHAT IS THE PURPOSE OF THIS DOCUMENT?

At St John's Hospice we're honest, we're analytical, we're straight forward – it's part of our ethos. This applies to how we look after your data.

Your ongoing support is invaluable to us. Without it, we cannot continue to care and support our patients and their families in our community.

We would like to keep you as a supporter and therefore we will ensure that we respect your data and only use the information you provide us with for the purposes for which you gave it.

Below is our fundraising promise to you, our supporter, event participant, donor and customer: we've included an outline of how, why and when we obtain and use your personal information and how we keep it safe and secure.

St John's Hospice is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your relationship with us as a supporter, event participant, donor or customer in accordance with the General Data Protection Regulation (GDPR).

St John's Hospice is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former supporters, event participants, donors or customers. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under the data protection legislation.

DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.

- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

- When you sign up for an event
- When you make a donation (this includes regular donation)
- When you donate to our retail shops
- When you join our lottery
- When you request fundraising materials
- When you purchase a St John's Hospice product; e.g. a leaf on our tree
- When you complete our contact preference form (whether online, within one of our shops or submission of a paper form)
- Whenever you sign up to an event on one of our partners' websites: e.g. JustGiving
- When you complete a Gift Aid declaration

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We will collect, store, and use the following categories of personal information about you:

Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.

- Date of birth
- Gender
- Next of kin and emergency contact information
- Bank account details and tax status information
- Location of employment or workplace
- Supporter motivation and affiliated status
- Complaints information
- CCTV footage and other information obtained through electronic means
- Photographs, video footage and quotes, with your permission.
- Information about your use of our online platforms
- Marketing contact consent status
- Donation amount and frequency (when donating via Direct Debit)

- Online page details and amounts
- Tax status
- Relevant medical details, dietary requirements, access requirements, self-exclusion declaration and additional support needs

We may also collect, store and use the following “special catnories” of more sensitive personal information:

Information about your health, including any medical condition, current diagnoses, encounters with hospice medical staff/services

- Safeguarding risks pertaining to mental health or criminal convictions

LEGITIMATE INTERESTS

A legitimate interest is most likely to be an appropriate basis where we use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if we can show there is an even more compelling benefit to the processing and the impact is justified.

We can rely on legitimate interests for marketing activities if we can show that how we use people’s data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object. The Hospice relies on legitimate interests for promoting its work to people on its database who have previously attended or expressed an interest in a Hospice event or who support the work of the Hospice by Volunteering. The Hospice considers this a proportionate response and, therefore, a legitimate interest. However, you can opt out of this anytime by contacting the Supporter Care team at the Hospice.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to, in the following circumstances:

- Business management and planning, including accounting and analysis
- To refer you to a designated solicitor to process your will writing request
- To perform a financial transaction, for example a donation, registration for an event or to process your lottery membership payment
- Gathering evidence for possible complaints or disciplinary hearings
- Dealing with legal disputes involving you or employees, workers amd contractors, including accidents on the hospice site/s
- Ascertaining your fitness to participate in a hospice-led event
- Complying with health and safety obligations
- To prevent fraud, money laundering and irresponsible gambling
- To monitor your use of our information and communication systems to ensure compliance with

our policies

- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- To conduct data analytics studies to review and better understand retention and attrition rates for service improvement and research
- To conduct data analytics studies to make our marketing campaigns more targeted and relevant to potential donors and customers
- To analyse and improve the services offered on our website
- To provide you with information (such as fundraising or campaigning activities), services or products you've requested or which we feel may interest you
- To process personal information and/or provide this to a third party for the purposes of marketing. This could be analysing demographics to inform our campaign and marketing strategies.

  For example:

  Age: Some campaigns would exclude supporters whose known age is not within the target audience.

  Gender: Gender is also used for some email promotions, like the Moonlight Walk emails.

  Previous interactions: A supporter's previous interaction with St John's Hospice is also used for targeting purposes. For example, a weekly lottery player would be prioritised for future lottery communications.

  To claim Gift Aid from HRMC: Personal information held by the Fundraising and Retail teams is used for the purpose of claiming Gift Aid on donations of goods made by supporters to our charity shops and E-bay and also on financial donations. We send information to HRMC in order to make these claims.

  To match information collected from you through different means or at different times. That could include using information collected online and offline, along with information obtained from other sources, including third parties and publicly available sources, to ensure that the information we hold about you is up to date and accurate. These include third parties such as BT OSIS, Post Office Address File and Experian Quick Address.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the agreement we have entered into with you, or we may be prevented from complying with our legal

obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

HOW WE STORE YOUR INFORMATION

Your personal information is stored electronically on our database indefinitely unless a supporter requests for it to be removed. Paper records of supporter, event participant, donor or customer information are destroyed after 3 years via a secure disposal company or if this information includes Gift Aid donations it will be destroyed after 7 years in line with HRMC regulations. Within this time your paper records are stored onsite for the first 12 months at St John's Hospice then transferred to our retail office at Edenvale to be stored in a secure storage room.

All photographic documentation is kept permanently for archival purposes and historic research.

If we hold data about you, you can ask us to delete that data and, in some circumstances, we will then do so. This is known as the right to erasure. You may sometimes hear it called the 'right to be forgotten'.

HOW DO YOU ASK FOR YOUR DATA TO BE DELETED?

You should contact St John's Hospice and let us know what you want erased. It is preferable to contact the Director of Income Generation; however any member of the Supporter Care team will be happy to assist.

A request can be verbal or in writing. We recommend you follow up any verbal request in writing because this will allow you to explain your concern, give evidence and state your desired solution. It will also provide clear proof of your actions if you decide to challenge the organisation's initial response.

When can you request erasure?

If any of the following apply to your data, we will erase it as soon as we can after you ask us to:

- The Hospice no longer needs your data
- You initially consented to the use of your data, but have now withdrawn your consent
- You have objected to the sue of your data and your interests outweigh our interests in using it
- We collected or have used your data unlawfully

St John's Hospice has a legal obligation to erase your data within 28 days.

DATA SHARING

In order to process our regular payment scheme such as the Lottery and regular giving we need to

share your information with our trusted third party providers. This is through secure online share portals and we have an agreement with our third parties regarding compliance.

- When large mailings are undertaken, St John's Hospice shares data with an external mailing house for the purpose of the mailing as a one off. The third party will supply the hospice with an agreement for the purpose of the data sharing and disposal.

EXTERNAL DATA COMPANIES

- From time to time we use external data cleansing companies to ensure our data is cleansed so that we hold accurate information and to help us better understand our supporter base. The third party will supply the hospice with an agreement for the purpose of the data sharing and disposal.
- We share data with HRMC for the collection of Gift Aid on donations.

We do not share data unless with third party suppliers with whom we are working for the benefit of the hospice.

If you need further information on erasure please visit the Information Commissioner's Office (ICO) website or call them on 0303 123 1113.

DATA PROTECTION

If you have any questions about this privacy notice or how we handle your personal information, please contact the Director of Income Generation. You have the right to make a complaint at any time to the ICO, the UK supervisory authority for data protection issues or the Fundraising Regulator.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

10: DEFINITIONS/GLOSSARY OF TERMS

1. Definitions

Where a word starts with a capital letter it will have a particular meaning in this Privacy Standard, as explained below.

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. The Hospice is the Data Controller of all Personal Data relating to the Hospice, Hospice Personnel and Personal Data used by the Hospice for our own operational purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Hospice Personnel: all employees, workers (including bank nursing staff), volunteers, trustees, agency workers.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access (e.g. a patient's NHS number). Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual

(for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Guidelines: the Hospice's privacy/GDPR related guidelines provided to assist in interpreting and implementing this Privacy Standard and any policies relating to data protection or information governance (see Appendix for the list).

Privacy Notices (also referred to as Fair Processing Notices): separate notices setting out information that may be provided to Data Subjects when the Hospice collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices, patient/family privacy notices or volunteer privacy notices) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

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

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions. Patient records are an example of Sensitive Personal Data.

Accessible health record (Access to Health Records Act 1990) – means any health record, which consists of information relating to the physical or mental health or condition of an individual made by or on behalf of a health professional in connection with the care of that individual. (Also includes certain educational records and accessible public records defined in Schedules 11 and 12 of the Data Protection Act 1998) – also see paragraph entitled Health Record below.

Application – means an application in writing by:

- The patient
- A person authorised in writing to make the application on the patient's behalf, .e.g. a solicitor with written consent from patient

- Where the record is held in England and Wales and the patient is a child, a person having parental responsibility of the patient
- Where the record is held in Scotland the patient is a pupil, a parent or guardian of the patient
- Where the patient is incapable of managing his or her own affairs, or where the patient has died, the patient's personal representative and any person who may have a claim arising out of the patients death – see Sections 5, 6 and 7 of this document

Author – means the professional, health or corporate who is or had responsibility and made entries to the data subjects record during the period to which the application refers.

Caldicott Guardian

This is an identified role within the organisation, and is held by the Head of Nursing & Quality. They are the "conscience" of the organisation when dealing with patient's personal information and its data management, but also have a strategic role which involves representing and championing Information Governance requirements across the organisation. Staff should seek the advice of the Caldicott Guardian where necessary.

Child – means an individual who has not attained the age of 16 years

Data - can be text, photographs, audio or video, electronic or manual and is information which:

- is being processed by means of equipment operating automatically in response to instructions given for that purpose
- is recorded with the intention that it should be processed
- is recorded as part of a 'relevant filing system' or with the intention that it should form part of a relevant filing system
- does not fall within the above but forms part of an 'accessible record'.

This may include databases, data files, research information, policies and procedures, audits, manuals and training materials, contracts and agreements, business continuity plans, back-up and archive data, applications and systems software, data encryption utilities, development and maintenance tools, computing hardware, including mobile and smart phones and tablets, printers, paper records including patient healthcare records and staff personal records.

Data controller - A person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

Data subject – means an individual who is the subject of the data or information or record

Data subject's consent – means any freely given, specific and informed indication of their wishes, by which the data subject signifies their agreement to personal data relating to them, being processed.

Health record – The Data Protection Act 1998 defines a health record as being any record which consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual. This includes all types of media, e.g. written, visual, electronic and audio records.

Health professional – as defined in the Data Protection Act 2018 means any of the following:

- A registered medical practitioner (includes any person who is provisionally registered under section 15 or 21 of the Medical Act 1983 and is engaged in such employment as is mentioned in subsection (3) of that section)
- A registered dentist as defined by section 53(1) of the Dentists Act 1984
- A registered optician as defined by section 36(1) of the Opticians Act 1989
- A registered pharmaceutical chemist as defined by section 24(1) of the Pharmacy Act 1954, or a registered person as defined by article 2(2) of the Pharmacy (Northern Ireland) Order 1976
- A registered nurse, midwife or health visitor
- A registered osteopath as defined by section 41 of the Osteopaths Act 1993
- A registered chiropractor as defined by section 43 of the Chiropractors Act 1994
- Any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 for the time being extends
- A clinical psychologist, child psychotherapist or speech therapist
- A (music / art) therapist employed by a health service body, e.g. Primary Care Trust
- A scientist employed by such a body as head of department
- Any person who is recognised by the organisation as a health professional, although they may not be registered e.g. a Nursing Assistant.

Holder – means health service body, such as a Hospice, Primary Care Trust, or Acute Trust that hold records

Information – in relation to a health record, means an expression of opinion about the patient including care detail

Information Asset Owner- This role is accountable to the Senior information Risk Owner (SIRO, see below) and is held by the Director of Finance & Resources at St John's Hospice. This role covers information governance of all information, not just patient information.

Personal data – means data which relates to a living individual who can be identified:

- from those data
- from those data and other information in the possession of, or likely to come into the possession of the Data Controller
- includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
- may also include opinions expressed by the data subject – additional guidance can be found in the Information Commissioners office document 'Data Protection Technical Guidance Determining what is personal data' v1.0 21.08.07

http://www.ico.gov.uk/upload/documents/library/data_protection/detailedspecialist_guides/personal_data_flowchart_v1_with_preface001.pdf

Processing – means

- Obtaining, recording or holding information or data, or carrying out any operation or set of operations on the information or data including:
- Organisation, adaptation or alteration or,
- Disclosure by transmission, dissemination or otherwise making available or,
- Alignment, combination, blocking, erasure or destruction

Relevant filing system (manual records) – means any set of information relating to individuals that is not automatically processed but is structured either by reference to individuals or by reference to criteria to individuals in such a way that specific information relating to a particular individual is readily accessible – e.g. paper records filed by name, date of birth, or allocated internal identification.

Sensitive personal data – means personal data as to the data subject's

- Racial or ethnic origin
- Political opinions
- Religious beliefs or beliefs of a similar nature
- Membership of a Trade Union
- Physical or mental health or condition
- Sexual life
- Criminal offences
- Criminal proceedings and convictions

SIRO (Senior Information Risk Owner)

This is held by someone at board level and has responsibility for understanding how the strategic business goals of the organisation may be affected by any information risks. The role looks at all possible risks not just of patient information. The Information Asset Owner is responsible to the Chair of the Board.

Staff – this encompasses staff, volunteers, sessional workers and those on placement at St. John's Hospice.

18: MANUAL RECORDING OF INFORMATION

Original Signed Document in Chief Executive's Office

19: DOCUMENT ACCESS TO STAFF

G drive at St John's Hospice, Lancaster

20: RELEVANT ASSOCIATED INTERNAL DOCUMENTS

SJ.HR 08 Information Governance

SJ. HR 41 Professional Behaviours at St John's Hospice

SJ.HR 13 Disciplinary Procedure

SJ.HR.74 Policy for the Retention, Destruction and Disposal of Records

21: SUPPORTING REFERENCE/EVIDENCE BASED DOCUMENTS

The Data Protection (Subject Access Modification (health) Order 2000
Access to Health Records Act 1990
Caldicott Report 1997
Computer Misuse Act 1990
Data Protection Act 1998 & 2018
Data Protection Good Practice Note: Charities and Marketing 2005
Freedom of Information Act 2000
Health and Social Care Act (section 60) 2008
Human Rights Act 1998
Mental Capacity Act 2005
Electronic Communications Privacy Act 1968
Public Interest Disclosure Act ("Whistle blowing") 1998
Public Records Act 1967
The report on Regulating fundraising for the future: trust in charities, confidence in fundraising regulation published on 22 September 2015 produced by a cross-party committee chaired by Sir Stuart Etherington.
The Information Commissioner's Office
The Fundraising Regulator

22: CONSULTATION WITH STAFF AND PATIENTS

Name:	Designation:	Date
Senior Management Team	:	February 2017

23: This document meets the requirements of the Equality Act 2010 in relation to Race, Religion or Belief, Age, Disability, Gender, Sexual Orientation. Gender Identity, Pregnancy & Maternity, Marriage and Civil Partnership, Carers, Human Rights and Social Economic Deprivation discrimination.

This document complies with the Care Commission Outcome Nos: 1 and 21

24: Checklist for the Review and Approval of Procedural Document

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Have the appropriate people been involved in the development of this document?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
	Has an Impact Assessment been completed for the policy content?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are supporting documents referenced?	Yes	
6.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	N/A	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done? (include in Team Brief / G drive)	Yes	
	Does the plan include the necessary training/support to ensure the compliance?	Yes	
8.	**Document Control**		
	Does the document identify where it will be held? (Authors responsibility)	Yes	
	Have archiving arrangements for superseded documents have been addressed?	Yes	
	Title of document being reviewed:		
9.	**Process to Monitor Compliance and Effectiveness**		

	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**Review Date**		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so is it acceptable?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes	

25: Equality & Diversity Impact Assessment Tool

<table>
<tr><th colspan="4">ASSESSMENT QUESTION AGAINST POLICY</th><th>YES/NO</th><th>COMMENT/ACTION POINT</th></tr>
<tr><td colspan="6">Does the policy, or any part of it (particularly any access criteria) discriminate on the grounds of any of the following criteria:</td></tr>
<tr><td>Age</td><td>No</td><td>Religion</td><td>No</td><td colspan="2" rowspan="4">If so please give further details:</td></tr>
<tr><td>Race</td><td>No</td><td>Sexual Orientation</td><td>No</td></tr>
<tr><td>Gender</td><td>No</td><td>Disability</td><td>No</td></tr>
<tr><td>Culture</td><td>No</td><td>Gender Identity</td><td>No</td></tr>
<tr><td colspan="4">Does the policy relate to the broader aims of St. John’s?</td><td>Yes</td><td></td></tr>
<tr><td colspan="4">Does the policy relate to other agencies within the community?</td><td>Yes</td><td></td></tr>
<tr><td colspan="4">Does it promote equality and enhance community relations?</td><td>Yes</td><td></td></tr>
<tr><td colspan="4">Does it influence relations between different groups?</td><td>Yes</td><td></td></tr>
<tr><td colspan="4">Could some groups be affected differently?</td><td>No</td><td></td></tr>
<tr><td colspan="4">Is there any evidence that some groups are affected differently?</td><td>No</td><td></td></tr>
<tr><td colspan="4">Has all existing data, research consultations, focus groups and analysis available of in-house information been used in preparing this policy?</td><td>Yes</td><td></td></tr>
<tr><td colspan="4">Is the impact of the policy likely to be negative?</td><td>No</td><td></td></tr>
<tr><td colspan="4">If so can the impact be avoided?</td><td>-</td><td></td></tr>
<tr><td colspan="4">Does is meet the relevant Equality and Diversity act?</td><td>Yes</td><td></td></tr>
<tr><td colspan="4">Can the policy be justified?</td><td>Yes</td><td></td></tr>
<tr><td colspan="4">Are there alternative ways of achieving the policy without the impact?</td><td>No</td><td></td></tr>
<tr><td colspan="4">Can we reduce the impact by taking different action?</td><td>No</td><td></td></tr>
<tr><td colspan="4">Has consultation taken place with those groups likely to be affected by the policy?</td><td>Yes</td><td></td></tr>
</table>

26: APPROVAL

Author: Sue McGraw **Job Title:** Chief Executive Officer **Date:** April 2021

Ratified: Chief Executive

Date: April 2021

Signed: Sue McGraw

Job Title: Chief Executive