Introduction

St Rocco's Hospice holds and processes information about its employees, patients, donors and other individuals for various purposes (for example, the effective provision of healthcare services, operating the payroll, managing donations/gift aid and to enable correspondence and communications.) To comply with the Data Protection Act 2018 (DPA18) and UK General Data Protection Regulation (UK GDPR) information must be collected and used fairly, stored safely and not disclosed to any unauthorised person. The DPA18 applies to both manual and electronically held data.

Compliance with Statutory Requirements

- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Data Protection Act 2018
- Environmental Information Regulations 2004
- UK General Data Protection Regulation
- Human Rights Act 1998

Related Policies / Procedures

- Confidentiality
- eMail Usage
- Incident Management & Reporting
- Information Assets
- Information Governance
- NHSx Records Management Code of Practice 2023
- ICO HR Data Retention Schedule 2021
- Data Security and Protection Toolkit
- Information Management
- Information Security
- Removable Media
- Staff Confidentiality Code of Conduct
- Subject Access Requests

Scope

This policy covers records held and processed by the hospice. The hospice is responsible for its own records under the terms of the Data Protection Act 2018 (DPA18) and it has submitted a notification as a Data Controller to the Information Commissioner.

The policy also applies to all individuals who are involved in processing information relating to hospice activities, particularly where sensitive data is recorded or stored.

Policy Statement

The lawful and correct treatment of personal information is vital to the successful operation of and maintaining confidence within the hospice and the individuals with whom it deals.

Therefore, the hospice will, through appropriate management, and strict application of the criteria and controls within the DPA18:

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Apply strict checks to determine the length of time information is held

- Ensure that the rights of people about whom information is held can be fully exercised under the act. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong information)
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards

Responsibility / Accountability

Notification to the Information Commissioner

The hospice has an obligation as a Data Controller to notify the Information Commissioner of the purposes for which it processes personal data. Notification monitoring within the hospice is carried out by the Senior Information Risk Owner (SIRO.) Individual data subjects can obtain full details of the hospice's data protection registration/notification with the Information Commissioner from the Information Governance Lead, or from the Information Commissioner's website on https://ico.org.uk/ESDWebPages/Entry/Z6965076

Hospice staff with Data Protection responsibilities

All queries about this hospice policy should be directed to the SIRO. Requests for access to patient's confidential medical records should be addressed to the Caldicott Guardian.

Requests for a patient subject access should be made to the Caldicott Guardian. Hospice staff requiring personal information should complete the appropriate form shown in the Subject Access Request policy and send it to the Human Resources Officer.

Data Protection Principles

The hospice, as a Data Controller, must comply with the six Data Protection Principles set out in the DPA18. In summary, these state that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Processing

"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- Organisation, adaptation or alteration of the information or data
- Disclosure of the information or data by transmission, dissemination or otherwise making available, or
- Alignment, combination, blocking, erasure or destruction of the information or data

Privacy Notices

Sometimes called a 'Fair Processing' Notice, any collection of personal data must satisfy the requirements of the fair processing condition set out in the first data protection principle. This includes paper or electronic application forms, telephone calls and surveys. An appropriate Privacy Notice is included wherever personal data is collected. This particularly applies to patient consent forms.

There is also a need to inform donors of any information held on them and how it may be used in relation to fundraising activities, gift aid administration. Information must be provided at the point the data is collected such as website or in shops.

The purpose of a Privacy Notice is to explain to the individual:

The identity of the organisation collecting his or her data:

- How the personal information which is provided will be used
- Any other information which the individual should be told in order to ensure the processing of his or her information is fair e.g.
    - a description of any other organisations the information may be shared with or disclosed to; whether the information will be transferred outside the UK
    - the fact that the individual can object to the use of his or her information for marketing
    - the fact that an individual can obtain a copy of his or her information

Ensure that the Privacy Notice is prominently displayed whenever used

Responsibilities of Individual Data Users

All employees of the hospice who record and/or process personal data in any form (called "Data Users" in this policy) must ensure that they comply with:

- the requirements of the DPA18 (including the data protection principles)
- the hospice's Data Protection Policy, including any procedures and guidelines which may be issued from time to time

A breach of the DPA18 and/or the hospice's Data Protection Policy may result in disciplinary action.

Consideration should be given towards contacting the Information Governance Lead for data protection advice concerning the following:

- when developing a new computer system for processing personal data - it may also be necessary to comply with the hospice's Information Asset Policy
- when using an existing computer system to process personal data for a new purpose as it may be necessary to notify an amendment to an existing registration in the hospice's Information Asset Policy
- when creating a new manual filing system containing personal data
- when using an existing manual filing system containing personal data for a new purpose

Accuracy of Data

Staff who have responsibility for handling any patient, donor, staff or other individual's information must ensure that it is accurate and as up to date as possible, as detailed in their job descriptions.

All staff members are responsible for checking that any personal information they provide to the hospice in connection with their employment is accurate and up to date e.g. change of address or name. The hospice cannot be held responsible for any errors unless the member of staff has informed the hospice about them.

Special Category Data

The hospice may from time-to-time process "sensitive personal data" relating to staff, patients, donors and other individuals. This sensitive personal data may include information which has incidentally come into the possession of the hospice. This type of information will not be routinely sought by the hospice.

In exceptional circumstances, the hospice may need to process information regarding criminal convictions or alleged offences in connection, for example, with any disciplinary proceedings or other legal obligations.

In circumstances where sensitive personal data is to be held or processed, the hospice will seek the explicit consent of the individual in question unless one of the limited exemptions provided in the DPA18 applies (such as to perform a legal duty regarding employees or to protect the data subject's or a third party's vital interests).

Data Security and Disclosure

All staff within the hospice are responsible for ensuring that:

- Any personal data which they hold is kept securely
- Personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party and that every reasonable effort will be made to see that data is not disclosed accidentally

Personal data must be kept securely and examples of how this may be done will include:

- Keeping the data locked in a filing cabinet, drawer or room
- ensuring that the data is password protected if the data is computerised or kept only on an encrypted removable device which is itself kept securely
- Any other appropriate security measures which are detailed in the hospice Information Governance Policies

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. If in any doubt, consult the SIRO, Information Governance Lead or Human Resources Officer.

Safe Havens

The term ‘Safe Haven’ is used to denote either a secure physical location or the agreed set of administrative arrangements that are in place to ensure security-classified, personal or other sensitive information is communicated safely and securely. Historically Safe Haven processes have been associated with the use of fax but now extend to cover email, telephone calls, internal and external post. The use of fax is now actively discouraged.

Safe Havens should be established, where:

- Information can be securely received and transferred
- Paper-based information is stored securely in approved containers, as soon as practical
- Computer terminals should not be on view or accessible to unauthorised persons
- All waste potentially containing security classified, personal or other sensitive information must be securely retained until it can be securely disposed of or destroyed
- Conversations discussing confidential personal or other sensitive information must be held where they cannot be overhead by unauthorised persons. The hospice has a duty of confidentiality when handling personal confidential data and a Safe Haven procedure should be established in order to maintain the privacy and confidentiality of personal confidential data

Data Subjects' Consent

It is hospice policy to seek and obtain express consent whenever practicable from individual data subjects for the main ways in which the hospice may hold and process personal data concerning them. This is to allow individuals an opportunity to raise any objections to any intended processing of their personal data. The hospice will consider any such objections but reserves the right to process personal data in order to carry out its functions as permitted by law. Legally, however, certain types of personal data may be processed for particular purposes without the consent of individual data subjects. Where this takes place, the hospice will ensure that individuals processing that data are required to justify their reasons for doing so in line with the DPA18 and the guidelines issued by the Information Commissioner.

Right of Access to Personal Data

Staff, patients, donors and other individuals have the right under the DPA18 to access any personal data that is being held about them either in an "automatically processable form" (mainly computer records) or in a "relevant filing system" (i.e. any set of information structured in such a way that specific information relating to a particular individual is readily accessible).They also have the right to request the correction of such data where they are incorrect. This is called a Subject Access Request.

CCTV

A number of CCTV cameras are present on the hospice sites, to assist with security for staff, other individuals and their property, and in accordance with the hospice’s 'notification' to the Information Commissioner. Disclosure of images from the CCTV system will be controlled and consistent with the purpose for which the system was established.

For example, it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be considered appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet. Images can be released to the media for identification purposes; this should not generally be done by anyone other than a law enforcement agency.

If you have any queries regarding the operation of or access to the CCTV system, please contact the hospice SIRO. If access is required in connection with ongoing disciplinary matters, permission should be sought from the Human Resources Officer or nominated deputy.

Email

It is permissible and appropriate for the hospice to keep records of internal communications, provided such records comply with the data protection principles. The appropriate use of email in the proper functioning of the hospice, and the limitations can be found in the hospice's Email Policy. All hospice staff should be aware that the DPA18 subject access right, subject to certain exceptions, applies to emails which contain personal data about individuals which are sent or received by hospice staff.

Disclosure outside of the United Kingdom (UK) or European Economic Area (EEA)

The hospice may, from time to time, need to transfer personal data to countries or territories outside of the UK or EEA (which is the European Union (EU) member states plus the European Free Trade Association (EFTA) countries of Iceland, Liechtenstein and Norway) in accordance with purposes made known to individual data subjects. For example, the names and contact details of members of staff at the hospice on a website may constitute a transfer of personal data worldwide. If an individual wishes to raise an objection to this disclosure, then written notice should be given to the hospice's SIRO.

Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the UK or EEA to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

The EU has the power to determine whether a third country (i.e. not an EU member state or an EFTA country) ensures an adequate level of protection for personal data by reason of its domestic law or the international commitments it has entered into. On 28 June 2021, the EU Commission adopted a decision on the UK's adequacy under the EU's General data Protection Regulation (EU GDPR).The European Commission has agreed that transfers of data to the UK from the EEA are valid under GDPR.

On the 12 October 2023, the UK formally adopted the use of a 'data bridge' mechanism to enable the safe transfer of personal data from the UK to the United States through the UK Extension to the EU-US Data Privacy Framework. The Secretary of State has determined that the UK Extension to the EU-US Data Privacy Framework does not undermine the level of data protection for UK data subjects when their data is transferred to the US. This decision was based on their determination that the framework maintains high standards of privacy for UK personal data.

The term 'data bridge' is the UK Government's preferred public terminology for 'adequacy' and describes the decision to permit the flow of personal data from the UK to another country without the need for further safeguards. Data bridges secure the free and safe exchange of personal data across borders, from the UK to another country.

Retention of Data

The hospice will hold different types of information for differing lengths of time, depending on legal and operational requirements, following which it will either be archived or destroyed. This will be done in accordance with the retention periods detailed in the hospice's Information Management Policy which is compliant with the:

- NHS England Records Management Code of Practice 2023
- ICO HR Data Retention Schedule 2021

Whilst the hospice is not directly subject to the Freedom of Information Act, this may change and it is a recognised best practice position.

Any hospice local retention policies will use the timescales detailed in the NHS Code of Practice

as a minimum. All data retention will comply with the 5th Principle of the DPA18.

Policy Monitoring and Review

This policy will be reviewed on a three yearly basis or more frequently if legislation or other hospice policies directly linked to this determine that the policy needs to be amended.

Audit plan

Spot checks on staff awareness of data protection principles will be carried out by a member of the group of people with data protection responsibilities to ensure compliance with the policy.

Changes to this policy

The hospice reserves the right to update or amend this policy at any time; please check on a periodic basis for the latest version