Data Protection Policy 155

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 (DPA) 2018 and UK General Data Protection Regulation information (UK GDPR) must be collected and used fairly, stored safely and not disclosed to any unauthorised person. The DPA applies to both manual and electronically held data.

Compliance with Statutory Requirements

- Data Protection Act 2018
- UK General Data Protection Regulation
- The Privacy and Electronic Communications (EC Directive) Regulations 2003.
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Environmental Information Regulations 2004
- Human Rights Act 1998

Related Policies / Procedures

- Confidentiality
- Email Usage
- Incident Management & Reporting
- Information Assets
- Information Governance
- NHSx Records Management Code of Practice 2021
- 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 all data held and processed by the hospice. The hospice is responsible for its own records under the terms of the DPA, and it has submitted a notification as a Data Controller to the Information Commissioner - Registration No. Z6965076

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 appropriate Data Protection legislation

- 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

1.1 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

1.2 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 by contacting the Hospice by any of the methods mentioned in Appendix 2 of this policy where you will be supported and guided through the processing of your request. Hospice staff requiring personal information can also contact the People's department and where possible, to speed up the process, complete the appropriate form shown in the ~~Subject~~ Access Request policy 159 and send it to the People's Department.

1.3 Data Protection Principles

The hospice, as a Data Controller, must comply with the seven 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') providing the appropriate legislated checks have been taken.

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

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 UK 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')

7. The controller is responsible for and must be able to demonstrate that they can evidence compliance with the principles listed above. This seventh principle being refers to as the accountability principle .

1.4 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

In addition to the provisions of UK GDPR and the DPA 2018, the Organisation also adheres to the principles which arose from the Caldicott Reports, which underpin the fundamental rules and regulations that guide a patient's confidentiality. They are the basic rules every healthcare personnel must follow to ensure there is no breach of confidentiality whatsoever.

· **Principle 1**: Justify the purpose(s) for using confidential information;

· **Principle 2**: Use personal confidential data only when it is necessary;

· **Principle 3**: Use the minimum necessary personal confidential data requires to meet your aim;

· **Principle 4**: Access to personal confidential data should be on a strict need-to-know basis and restricted to those who should have access to it;

· **Principle 5**: Everyone with access to personal confidential data should be aware of their responsibilities;

· **Principle 6**: Comply with the law; and

· **Principle 7**: The duty to share information can be as important as the duty to protect patient confidentiality.

· **Principle 8:** Inform patients and service users about how their confidential information is used

Data which has been anonymised, where there is no mechanism to redetermine the data subject, is no longer considered to be protected within the data protection legislation. However, if the Hospice uses pseudonymised data, where there is a mechanism to reidentify a data subject, for example, by the use of an identifying system, then that data must be considered to fall within the remit of this policy.

1.5 Privacy Notices

Any collection of personal data must satisfy the requirements of the fair processing condition set out in the first data protection principle. This includes, but is not limited to paper or electronic application forms, telephone calls and surveys and CCTV images An appropriate Privacy Notice is included wherever personal data is collected. This applies to data collected such as patient consent forms, health records, employee documentation and website use

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

For example:

- 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 and in the relevant place. E.g., employees can expect to be given access to their Privacy Notice when they take up a role whilst users of the Hospice website will find the Privacy Notice visible from our Home page.

1.6 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.

Changes to how we process data

Consideration should be given towards contacting the SIRO for data protection advice concerning, for example, 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

The most straightforward was to initiate change is to follow the guidance offered within the Data Impact Assessment Policy (insert link here).

1.7 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.

1.8 Special category Data

The hospice may process "sensitive personal data" relating to staff, patients, donors and other individuals. This sensitive personal data is referred to as Special Category 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 Special Category 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).

Definitions:

Personal Data

Personal data is information relating to living persons who can be identified, or who are identifiable, directly from the information we are processing, or who can be identified from that information in combination with other information.

The Information Commissioner's Office refers to a name as being the most common means of identifying someone. Whether any potential identifier identifies an individual depends on the context. A combination of identifiers may be needed to identify an individual.

The UK GDPR provides a non-exhaustive list of identifiers, including:

· name;

· identification number;

· location data; and

· an online identifier. 'Online identifiers' includes IP addresses and cookie identifiers which may be personal data.

Special Category data

Sensitive Personal Information is known as Special Category Data. Special category data is personal data that needs more protection because it is sensitive and the risk to the data subject is considered to be greater if there should be any data breach or incident involving the data.

The UK GDPR defines special category data as personal data:

· revealing racial or ethnic origin;

· revealing political opinions;

· revealing religious or philosophical beliefs;

· revealing trade union membership;

· genetic data;

· biometric data (where used for identification purposes);

· concerning health;

· concerning a person's sex life; and sexual orientation.

6.9 **Lawful Basis for processing Personal Data**

The first principle under Article 5 requires that you process all Personal Information, whether personal data or special category data lawfully, fairly and in a transparent manner. Processing is only lawful if you have a lawful basis to apply to the processing undertaken for the Organisation.

If no lawful basis applies to our processing, the processing will be unlawful and in breach of the first principle. Individuals have the right to erase personal data which has been processed unlawfully.

There are six lawful bases we can use to process Personal Data. When selecting the correct basis, the choice will be from UK GDPR Article 6, which outlines the following reasons for processing:

(a) **consent**: the individual has given clear consent for you to process their personal data for a specific purpose;
(b) **contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract;
(c) **legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations);
(d) **vital interests:** the processing is necessary to protect someone's life;
(e) **public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law;
(f) **legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's

personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

To choose the correct legal basis you should consider why you want to process the data and select the appropriate basis. If you feel uncertain about which of the bases to select, you should discuss this with the SIRO.

6.10 Lawful Basis for processing Special Category Data

The Hospice recognises that Special Category Data requires additional protection, as it has the potential to reveal sensitive aspects relating to our individual data subjects. This means that when we process any special category details a second level of protection must be assigned. The conditions applicable to Special Category Data are outlined in UK GDPR Article 9.

They are:
(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

If relying on conditions (b), (h), (i) or (j), you must also meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

Before processing any sensitive Personal Information, staff must notify the Information Governance lead, and/or Data Protection Officer of the proposed processing, so they may assess if the processing complies with the criteria noted above.

Special category data will not be processed until:

- the assessment above has taken place; and
- the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

In relation to special category data, we will comply with the procedures set out in this policy to make sure that it complies with the data protection principles.

6.11 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.

6.12 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

6.13 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.

6.14 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 and full details of how to proceed with such a request can be found within the Access Request policy & procedure 159.

..\..\..\Group1 Policies-Corporate, Finance, IG & IT\(G)Access Request Policy 159 Edn2 Vrn1 Apr 2025.pdf

6.15 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 be done by anyone other than a law enforcement agency.

The CCTV Policy in full may be found on the Hospice K drive under Policies & Procedures, Group 1 policies Corporate, Finance, IG & IT

..\..\..\Group1 Policies-Corporate, Finance, IG & IT\(G)Access Request Policy 159 Edn2 Vrn1 Apr 2025.pdf

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.

1.16 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. Therefore, all data processors must be respective in their communications and remain mindful at all times that all data may ultimately be seen by the data subject so a professional manner should be engaged at all times.

The Hospice is privileged to work with vulnerable service users who have the right to compassionate professional data support.

1.17 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 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.

As this requires specific consideration of current legislation and the wording of contractual terms, any data transfer which is known to be routed through, or potentially involves international transfer should be discussed with the SIRO and the DPO.

Transfer risk assessments are not something which the general policy user would determine. The SIRO would make those decisions

Contemporary guidance can be found here. International data transfer agreement and guidance | ICO

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/

1.18 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:

- NHSx Records Management Code of Practice 2021
- ICO HR Data Retention Schedule 2021

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.

Staff training requirements

Staff Group	**Training Method:** Email Cascade (Awareness) eLearning/Workbook Practical Assessment Group Training Session	Facilitator	Target Completion Date
Administration	Email Cascade	SIRO	Within 10 working days of ratification
Clinical Teams(including Therapies & Family Support)	Email Cascade	SIRO	Within 10 working days of ratification
Domestics	Email Cascade	SIRO	Within 10 working days of ratification
Kitchen	Email Cascade	SIRO	Within 10 working days of ratification
Maintenance	Email Cascade	SIRO	Within 10 working days of ratification
Medical Team	Email Cascade	SIRO	Within 10 working days of ratification
Volunteers	Email Cascade	SIRO	Within 10 working days of ratification

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 policy.

Definitions

As contained within this policy document.

Appendix 1 - EEA Countries

The 8th Principle of the Data Protection Act 1998 prohibited the transfer of personal information to countries or territories outside the European Economic Area (EEA). (Currently the EEA consists of the 27 European Union member states and 3 other states)

The **European Union** states are:

Austria
Belgium
Bulgaria
Croatia
Republic of Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden

Although the six data protection principles in DPA18 do not include a similar statement, any such transfers are still regarded as restricted. The ICO has issued guidance on such transfers:

Restricted Transfers

Under Chapter V of the GDPR, controllers and processors cannot transfer personal data outside of the EEA (to so-called 'third countries), unless adequate levels of data protection can be ensured. This was also the position under the law preceding the GDPR.

Appendix 2 – Contacts details

To contact the Hospice Senior Information Risk Owner (SIRO):
via email: InformationGovernance@stroccos.org.uk
by post: Senior Information Risk Owner, St Rocco's Hospice, Lockton Lane, Bewsey, WA5 0BW, Warrington

To contact the ICO in the UK about a complaint, you can call their helpline at 0303 123 1113 (Monday to Friday, 9am to 5pm) or use their live chat feature on their website, according to the ICO website.

Here's a more detailed breakdown of how to contact the ICO:

- **Helpline:** You can call the ICO's helpline on 0303 123 1113.
- **Live Chat:** Start a live chat with an advisor on the ICO website.
- **Email:** You can email the ICO at icocasework@ico.org.uk.
- **Website:** Visit the ICO website for information on making a complaint and accessing complaint forms.
- **Social Media:** You can also find the ICO on social media.
- **Textphone:** If you use a textphone, dial 18001 followed by 0303 123 1113.
- **By Post:** If you have supporting evidence in hard copy, you can print out the form and post it to them.
- **Complaints about the ICO:** If you have a complaint about the ICO, you can find information on how to complain about them on their website.
- **Compliments:** If you have a compliment for the ICO, you can also let them know.