ST CATHERINE'S HOSPICE

Information Governance Policy [incorporating Data Protection Policy]

Document Control Table

Document Title:	Information Governance Policy (incorporating Data Protection policy)
Document Ref:	POL 18
Author (name and job title):	Jane Abbott (Head of Quality & Data Protection)
SMT sponsor:	Eric Norman (Director of Finance, and SIRO)
Members of stakeholder group for this review:	Eric Norman (Director of Finance, and SIRO) Patricia Brayden (Medical Director, and Caldicott Guardian) Richard Warner (Fundraising Insight Manager, and member of IG Group) Paul Rooney (ICT Manager, and member of IG Group) Jane Whitehurst (Consultant and member of IG Group)
Target audience: - all staff & volunteers - staff only - clinical staff only - other (please specify)	All staff and volunteers
Key words:	
Version Number:	3
Document Status:	Approved
Date originally approved:	22 April 2016
Approved By:	Giles Tomsett, Chief Executive
Effective Date:	April 2016
Date of last review:	July 2018
Date of next review:	July 2020

Amendment History

Version (& date created)	Date of review / amendment	Author	Notes on revisions (inc reason)
CL-30 Policy on Confidentiality, Communication, & Clinical Information Management (Sept 2012)	April 2016	P Brayden, S Pearce, G Starnes	CL-30 superseded by POL 18 (also see Records Management Policy POL 30)
POL 18 v1 (April 2016)	April 2017	J Abbott	Appendix II added - *Guidance for managers on how to deal with a person connected to the hospice coming under our care or dying under our care* (April 2017)
POL 18 v2 (April 2017)	July 2018	J Abbott	Reviewed and changes

			made in line with GDPR and DP Act 2018; DP Policy merged with IG Policy.

Associated Documents

Media Policy
Records Management Policy
Mobile Devices Policy
Risk Management Policy
ICT policy and manual

References

1.NHS Data Security and Protection Toolkit
https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit

2. The Data Protection Act (2018)
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

3. Health & Social Care Act 2008
http://www.legislation.gov.uk/ukpga/2008/14/contents

4. Confidentiality: NHS Code of Practice
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

5. Records Management: NHS Code of Practice
https://www.gov.uk/government/publications/records-management-nhs-code-of-practice

6. Information Security Management: NHS Code of Practice
http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf

7. Human Rights Act 1998.

Contents

1. Purpose

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in corporate governance, service planning and performance management.

The purpose of this policy is to ensure a robust governance framework for information management, so that StCH can maintain the confidentiality, integrity, security and accessibility of data, information and processing systems. The framework will:
- ensure that all staff and volunteers working for or on behalf of StCH, and all third parties providing services to or for StCH, understand and comply with relevant legislation, including the Data Protection Act 2018
- enable all staff and volunteers to have confidence that they are processing personal and confidential data legally and ethically and with due regard to the wishes of our patients, their families and our donors.

StCH monitors its information governance controls through the NHS Data Security and Protection Toolkit, which is a self-assessment tool designed to ensure compliance with legal and regulatory requirements of information handling. The Toolkit covers:

- information governance management
- confidentiality and data protection assurance
- information security assurance
- incident management and continuity planning

2. Scope of policy

This policy applies to

- all information, information systems, networks, applications, and locations of StCH
- all staff employed by or working on behalf of StCH, third parties supplying goods and services to StCH, and all volunteers.

3. Definitions

- *Service users* - anyone using a service provided by StCH; which might include patients, families, carers
- *Data* - words, numbers, etc without context (and therefore without meaning)
- *Information* - collection of data put into context to give it meaning
- *Data integrity* - maintaining and assuring the accuracy and consistency of data over its entire life-cycle
- *Data Controller* – the person, authority or organisation that determines the purposes and means of the processing of personal data
- *Data Processor* – the person, authority or organisation that processes personal data on behalf of the data controller
- *Processing* – any operation which is performed on personal data or sets of personal data; the term ‘operation’ includes actions such as collection, recording, organisation, storage, adaption or alteration, use, disclosure by transmission or dissemination or otherwise making available.
- *Personal data* – any information relating to an indentified or identifiable natural person; an identifiable natural person is one that can be identified either directly or indirectly by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to that natural person.
- *Special category data* - broadly similar to the concept of sensitive personal data under the 1998 Act. Special category data is more sensitive, and so needs more protection. For example, information about an individual’s race, ethnic origin, politics,

religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation.

- *Senior Information Risk Owner (SIRO)* - senior person within an organisation responsible for ensuring the organisation's information risk is identified and managed, and that appropriate assurance mechanisms exist.
- *Caldicott Guardian* - senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.
- *Data Protection Lead* - person responsible for ensuring the promotion of data protection compliance and best practice in an organisation. This involves setting and maintaining standards, and establishing appropriate procedures across all departments and functions.

4. Policy statement & aims

The aims of this policy are to:

- Maximise the value of organisational assets by ensuring that data is
  - held securely and confidentially
  - obtained fairly and lawfully
  - recorded accurately and reliably
  - used effectively and ethically
  - shared and disclosed appropriately and lawfully
- Protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental.

There are four key interlinked strands to this policy:

4.1 Openness

- Non-confidential information about the Hospice and its services is available to the public through a variety of media, eg the Hospice website and Hospice publications.
- Patients should have access to information relating to their own healthcare, their options for treatment and their rights as patients.
- The Hospice will have clear procedures and arrangements for liaison with the press and broadcast media.

4.2 Legal Compliance

- The Hospice will establish and maintain policies and procedures to ensure compliance with the Data Protection Act 2018 (see below for key details) and the Access to Health Records Act (including responding appropriately to data subject access requests – see Appendix II of Records Management Policy)
- The Hospice regards all identifiable information relating to patients, carers, staff, volunteers and supporters as confidential except where exemptions can be applied (eg where there is a legal or ethical obligation to share such information).
- Service users and supporters will be informed of the purpose for which information is being collected and stored and who may access it; direct consent will be sought where needed for the collection, processing and disclosure of data.
- The Hospice will establish and maintain policies and procedures for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (eg Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

Data Protection Act (2018) – summary of legislation relevant to the protection and use of person identifiable data

The Act lays out six data protection principles governing the processing of personal data:

1. Processing must be lawful, fair and carried out in a transparent manner
2. Personal data to be collected for specified explicit and legitimate purposes and not further processed for incompatible purposes.
3. Personal data to be adequate, relevant and limited to what is necessary for the purposes for which they are processed
4. Personal data to be accurate and where necessary kept up to date. Every reasonable step must be taken to rectify any relevant inaccuracies without delay.
5. Personal data to be kept in a form that allows identification of data subjects for no longer than is necessary for the purposes for which it is processed. The data may be archived for longer periods but only if in the public interest or for scientific, historical research or statistical purposes.
6. The data controller to be responsible for and to be able to demonstrate compliance with the principles above.

The Act also sets out the rights of individuals over their data:

a. The right to be informed – about the collection and use of their personal data
b. The right of access – if someone asks they must be told free of charge (within a month) what data is held, for what purpose and with whom it will be shared
c. The right to rectification – data to be corrected within a month
d. The right to erasure – right only applies in specific circumstances, primarily where the individual withdraws consent and there is no overriding legitimate interest for continuing to hold or process that individual's data
e. The right to restrict processing – if data is inaccurate or no longer needed for those purposes
f. The right to data portability – to obtain and reuse their personal data
g. The right to object – initially to direct marketing but now extended to any processing based on legitimate interests
h. Rights concerning automated decision making and profiling – no 'significant decision' based solely on automated processes, can ask for any automated decision or evaluation of personal aspects to be reconsidered.

NB. StCH recognises its duty to uphold these rights and will consider how best to do so on a case by case basis.

4.3 Information Security

- Systems will be established and maintained to ensure that corporate records, including healthcare records, are available and accessible at all times.
- The Hospice will establish authorisation procedures for the use and access to confidential information and records.
- The Hospice will establish and maintain policies for the effective and secure management of its information assets and resources.
- The Hospice will undertake annual assessments and audits of its information and IT security arrangements.
- The Hospice will promote effective confidentiality and security practice to staff and volunteers through policies, procedures and training.
- The Hospice will establish and maintain incident reporting procedures which will include the monitoring and investigation of reported instances of actual or potential breaches of confidentiality and security.

4.4 Information Quality Assurance

- Managers are responsible for the quality of information within their services, and are expected to continuously seek to improve the quality of the information.
- Wherever possible, information quality should be assured at the point of collection.
- The Hospice will undertake annual assessment and audits of its information quality and records management arrangements.

5. Accountability and responsibility

Chief Executive is responsible for:
- appointing SIRO and delegating appropriate responsibility and authority to him/her
- appointing Caldicott Guardian.

SIRO (currently Director of Finance) is responsible for:
- ensuring the organisation's information risk is identified and managed, and that appropriate assurance mechanisms exist
- acting as advocate for information governance risk on the Board.

Caldicott Guardian (currently Medical Director) is responsible for:
- providing advice and guidance in the use and sharing of service user information
- approving, monitoring and reviewing protocols governing access to person identifiable information by staff within the Hospice and by relevant other agencies
- overseeing the control of access to and disclosure of healthcare records.

Data Protection/Information Governance Lead (currently Head of Quality & Data Protection) is responsible for:
- ensuring implementation of this policy
- ensuring sufficient resources are provided to support the requirements of this policy
- ensuring the promotion of data protection compliance and best practice in an organisation

Information Governance Group is responsible for overseeing day-to-day information governance issues
- developing & maintaining policies, procedures and guidance
- coordinating and raising awareness of IG throughout StCH
- providing regular reports on IG issues to the Board via the Quality Committee
- ensuring appropriate IG training is provided and accessed by staff.
- monitoring actual or potential reported information security incidents within the organisation

Information Asset Owners are responsible for:
- oversight of management of the information assets assigned to them (including the security and integrity of the data held therein).

Information Asset Administrators are responsible for:
- Day-to-day management of information assets assigned to them, including administration of any day-to-day changes required to the application, and provision of training to ensure all users are competent to use the application.

Managers are responsible for:
- ensuring that the policy and its supporting procedures and standards are built into local processes and that there is ongoing compliance
- ensuring that all staff job descriptions contain relevant responsibility for information security, confidentiality and records management
- ensuring their staff undertake mandatory information governance training

- ensuring any volunteers working with their team understand their responsibilities with respect to information governance
- the security of the physical environment where their team operates and where information is processed and stored.

All staff and volunteers are responsible for:
- complying with this policy and its supporting procedures, including maintenance of data confidentiality and data integrity
- maintaining the operational security of the information systems they use
- ensuring they complete any training as required.

6. Procedure

See *Appendix I Information Management and Security Framework*

7. Dissemination

This policy will be circulated to all staff by email when it is first issued and when it is updated. New staff joining the Hospice will be made aware of the policy as part of their induction.

Managers are responsible for ensuring that all staff are aware of the policy, know where to find it and understand their role in adhering to it. Managers will use team meetings, 1:1s and other appropriate routes to do this.

Managers are responsible for ensuring that their staff have completed the relevant training in order to understand and implement the policy, and are supported by information on compulsory training attainment provided by HR.

Information about the policy will also be included in the next available staff newsletter and shared with managers at the next available managers update session.

Staff who manage volunteers will be responsible for making those volunteers aware of the policy.

8. Monitoring and review

The Information Governance Group will audit the implementation of this policy and its associated procedures, including the development of an appropriate 'information governance aware/sensitive culture' across the organisation. Specific IG-focused audits will follow the requirements of the DPST Toolkit and will include reviews of:
- IG training compliance
- data collection, data validation and data quality
- access to confidential information.

Audit results will be reviewed by the Information Governance Group. Summary reports will presented as part of IGG quarterly reports to SMT and to the Quality Committee.

This policy will be reviewed every two years, or earlier if internal factors or changes to legislation deem it necessary.

Policy Impact Assessment

The impact assessment is used to ensure

- that we do not inadvertently discriminate as a service provider or as an employer
- that the information governance implications of any changes in the way we work, implicit in new policies, are considered and addressed appropriately.

To be completed and attached to all policies when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Equality Impact**		
a.	Does the policy affect one group more or less favourably than another on the basis of - race - ethnic origin - nationality - gender - culture - religion or belief - sexual orientation (including lesbian, gay & bisexual people) - age - disability (eg physical, sensory or learning) - mental health	N	
b.	If potential discrimination has been highlighted, are any exceptions valid, legal and/or justifiable?	N/A	
c.	Is the impact of the policy likely to be negative? If so, can the impact be avoided or reduced?	N	
2.	**Information Governance Impact**		
a.	Is the policy (or any of its associated procedures) likely to have an adverse impact on: - information quality - information security - confidentiality - data protection requirements	N	
b.	If so, have these issues already been raised with the Information Governance Group? What action has been agreed?	N/A	

For advice in respect of answering the above questions, please contact any one of the following:

Caldicott Guardian (StCH Medical Director)

Senior Information Risk Owner (StCH Finance Director)

Head of Quality & Data Protection

Services Information Coordinator

Appendix I

Information Management and Security Framework

Information takes many forms and includes:
- data stored on computers, CDs, DVDs, USB memory sticks and other mobile devices, and also stored remotely
- data transmitted across networks and sent by fax
- printed and handwritten information
- information shared in face-to-face conversation and over the telephone.

Data represents an extremely valuable asset and to ensure integrity the Hospice must safeguard accuracy and completeness by protecting against unauthorised use/disclosure, modification or interruption.

The key issues addressed by this framework are:

- **Confidentiality** Data is secure and access is confined to those with specified authority to view the data
- **Integrity** All system assets are operating correctly according to specification and in the way the current user believes them to be operating
- **Availability** Relevant information is delivered to the right person when it is needed

Detail	Associated policy/ procedure/guideline	Responsibility
1. Information Governance/Information Security Awareness Training • Security awareness training is included in the staff induction process • Information Governance training is included in the compulsory training programme for all staff and volunteers	Staff induction procedure Training & Development Policy	IT Team HR Team/ Volunteering Team
2. Contracts of Employment • All contracts of employment will contain a confidentiality clause • Information security expectations of staff will be included in appropriate job descriptions • All contracts with a third party supplier of goods or services will contain a confidentiality clause and an undertaking that any information obtained during the course of performing the contract is confidential and shall only be used for the sole purpose of the execution of the contract.	HR policies Contracts management procedure SLA template for consultants/temps	HR Dept HR Dept/All managers Contracts Officer HR
3. Security control of assets • Each information asset (hardware, software, IT application or data) will have a named information asset owner who will be responsible for the security and integrity of that asset. • A register of all information assets and their owners will be maintained by the Information Governance Group	IT Policy / IGG ToR	IT Team & IG Group IG Group
4. User access controls and monitoring • Access to information will be restricted to authorised users who have a bona-fide business need to access the information • An audit trail of system access and data use by staff will be maintained and reviewed on a regular basis where the system is capable of providing this.		IAOs IAOs
5. Computer access control • Access to computer facilities will be restricted to authorised users who have a business need to use the facilities. HR will	IT Policy	IT Team + IAOs

provide IT with details new staff and line managers will provide authorisation for changes to access and systems privileges. • Access to data, system utilities and programme source libraries will be controlled and restricted to those authorised users who have a legitimate business need, eg systems or database administrators.	IT Policy	IT Team
6. Security of IT system • In order to minimise loss of or damage to assets, key IT equipment will be physically protected from threats and environmental hazards • All items of computer equipment will be recorded on the Hospice's register of IT assets • Computer screens should not normally be visible from areas accessed by the public; wherever possible screen savers should be applied. • Server rooms will be kept secure with doors and windows closed or locked when unattended.	IT Policy	IT Team IT Team All managers IT Team
7. IT system management • Responsibilities will be appropriately assigned for the management of IT systems. These will include the management, monitoring and auditing of access to IT systems and the timely management of starters and leavers and those changing job role.	IT Policy	IT Team + HR Dept
8. Computer and network procedures • Management of computer and networks will be controlled through standard documented procedures that have been authorised by the IT Team. • A register of users with 'on behalf of StCH' access to third party websites/systems will be maintained and managed by the HR Department. Managers are responsible for controlling access rights and notifying HR Department of changes.	IT Policy	IT Team HQDP + all managers

9. User media • Staff using mobile devices must comply with the Hospice's Mobile Devices Policy	Mobile Devices Policy	All staff
10. Access to internet and email • The Hospice will ensure awareness of internet and email policies, including those with reference to use of social media.	IT Policy	HR
11. Information Risk Assessment • All key/critical information systems will be subject to periodic risk assessments carried out by systems managers/administrators	Risk Management Policy	Managers
12. Business continuity & disaster recovery plans • The Hospice will ensure that continuity and recovery plans are in place for all IT mission critical information, applications, systems and networks	Business Continuity/Disaster Recovery Policy	IT Manager
13. Data quality & validation • The Hospice will ensure that there is up-to-date, complete and accurate data within information systems that support operational and clinical decision-making	Records Management Policy	IAOs
14. Information security incident management • All information security incidents (including near misses) will be reported and investigated through the Hospice's incident management policy and procedure • All significant information security incidents will be reported to the relevant regulatory authority via the DSPT Toolkit	Incident Management Policy IG Policy – Appendix III Procedure for reporting significant IG breaches	Managers HQDP
15: Volunteers • All volunteers will sign a confidentiality clause as part of the application/selection process • Information security and confidentiality expectations of volunteers will be included in appropriate role profiles	Volunteers Policy	Volunteering Development Manager

Appendix II

Processing of Personal Data

Background/rationale

In order to ensure compliance with the Data Protection Act 2018 (DPA) it is necessary to establish a framework for recording:

- what personal data is collected
- how the data is processed
- how the data is stored
- with whom (organisations or individuals) the data is shared and the lawful reason for that sharing
- the justification under the DPA 2018 for the processing.

StCH Framework

The framework developed by StCH consists of a process map for each information asset identifying:

- the type of data being processed
- the processes undertaken
- the department or external organisation where any data is transferred.

The process map is supported by a description of the data being collected and processed, where and how that data is stored, the length of time the data is held and the justification for our processing under the terms of the DPA.

The process mapping and supporting information is available to all staff at all times: P:\Governance\Quality and Safety\Information Governance Group\GDPR

Responsibilities

Information Asset Owners (supported by Information Asset Administrators) are responsible for:
- maintaining their respective process maps and supporting documentation to ensure its continued accuracy
- developing means to check that the personal data processing information held for their information asset is an accurate reflection of day to day activity.

Information Governance Group is responsible for:
- monitoring the application of the DPA including any additional guidance or rulings issued by the ICO and to ensure StCH responds appropriately to any legislative or regulatory developments

- overseeing a programme of data processing and protection audits to gain assurance as to the level of StCH compliance with the DPA and to direct any required remedial activity.
- ensuring any significant data breaches are reported in accordance with the DPA (see Appendix III).

Appendix III

Procedure for reporting significant data breaches

1. Purpose

The objective of this procedure is to ensure that any significant data breach (as defined by the Information Commissioner's Office – see below) is reported to the ICO within 72 hours after the breach has occurred.

2. Scope

This procedure applies to all personal data processed by StCH – in any form and in any location where StCH (or someone working for or on behalf of StCH) is working.

3. Definitions

A **personal data breach** can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed. Breaches can be the result of both accidental and deliberate causes.

A **significant data breach** is one that seriously interferes with the rights and freedoms of one or more data subjects. Organisations need to focus on the potential negative consequences for individuals, and consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. Breaches can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.

For more information about what a personal data breach is see:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

4. Procedure

4.1 All information governance incidents and/or data breaches (actual or suspected) should be reported in the first instance via Datix. All potential data breaches will be reviewed at the earliest opportunity by the Head of Quality & Data Protection (or by their nominated deputy).

4.2 Once an incident is reported via Datix, the HQDP (or their nominated deputy) will establish whether a personal data breach has occurred.

4.3 If it is deemed to be a personal data breach, the HQDP (or their nominated deputy) will review it to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk (ie it is a significant data breach) then the ICO must be notified; if it's unlikely, then there is no need to report it to the ICO. However, the decision not report must be justified and recorded in the Datix record.

4.4 The ICO can be notified either by phone or online:
Phone: 0303 123 1113 Mon-Fri 9.00-4.30. The following information will be required:

- what has happened;
- when and how you found out about the breach;
- the people that have been or may be affected by the breach;
- what you are doing as a result of the breach; and
- who we should contact if we need more information and who else you have told.

Online form is available here
https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

It is the responsibility of the HQDP (or their nominated deputy) to notify the ICO.

4.5 Significant data breaches should be notified to the ICO within 72 hours. If there is a delay of more than 72 hours in reporting the breach, the reason for the delay must also be reported.

Appendix IV

Data Protection Impact Assessment Template

Electronic copy of this form is available at: P:\Forms & Templates\Data Protection Impact Assessment template (v1 Sept 2018).dotx

Step 1. Identify the need for a DPIA
Explain broadly what this project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
Step 2. Describe the processing
Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of StCH's relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues or public concern you should factor in? Are you signed up to any approved code of conduct or certification scheme (if any have been approved?)
Describe the purposes of processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of processing – for StCH, more broadly?
Step 3: Consultation process
Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within StCH? Do you need to ask your processors to assist (if applicable)? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality
Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply (if applicable)? How do you safeguard any international transfers (if applicable)?
Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** (eg remote, possible or probable)	**Severity of harm** (eg minimal, significant or severe)	**Overall risk** (eg low, medium or high)

Step 6: Identify measures to reduce risk				
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risks in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** (eg eliminated, reduced, accepted)	**Residual risk** (low, medium, high)	**Measure approved** (Yes/no, and by whom)

Step 7: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:		
Residual risks approved by:		
DPO advice provided:		
Summary DPO advice:		
DPO advice accepted or overruled by:		If overruled, explain reasons:
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix V

Guidance for managers on how to deal with a person connected to the hospice coming under our care or dying under our care

St Catherine's Hospice has been established in the local community for over 30 years and the majority of our colleagues, volunteers and long-standing supporters live locally. Caring for people we know or who have a significant connection with the hospice is becoming increasingly common. It can be a privilege to care for someone you know well, but can also be emotionally demanding, and can mean that colleagues require extra support, both while caring and afterwards. At the same time, when people known to the hospice community - and who may be friends as well as colleagues - come under our care, and die under our care, it can be difficult for us to know how to handle issues like communication and confidentiality and boundaries can feel a bit blurred.

This document is intended for managers to help them handle these difficult situations and to ensure that we meet our obligations to patients, their relatives, employees and volunteers in our teams. Bearing in mind that each individual is different and that dealing with illness, death and bereavement is deeply personal, it is not possible to give a protocol or set of rules for managing each individual situation. However, there are some important principles to adhere to and to consider. This document aims to answer some of the common questions managers might have, to give them some idea of what they should consider and how to get further advice and support. If you have any questions about this, please speak to your line manager.

Areas covered are:

When someone you or your team know has been referred to St Catherine's

1. A person I know socially or family member has been referred to the hospice. Do I need to do anything different?

This is a difficult situation and you need to consider the impact on you, as well as the impact on the person close to you and on your colleagues.
Consider whether your connection to this person makes it hard for you to do your job. If it does, or you need extra support, talk to your manager.

Consider reminding your friend or family member that StCH keeps clinical records confidential and that information held in their records will not be shared outside the team providing care. You may need to explain that you cannot access their record even if they ask you to.

2. A relative or close friend of someone in my team is under the care of StCH. What do I need to consider?

This is a difficult situation and there are a number of things to consider and, if necessary, discuss with the person in your team. These include:

- How is this affecting the person in your team? If they need additional support, refer to the Wellbeing Resources on the Intranet and get advice from the HR Team or Volunteering Team if needed.
- Might your team member be expected to give clinical care to their relative or friend? How close is the relationship and would this cause difficulties for either party or for other clinical colleagues? If it would, consider making special arrangements by asking colleagues to help and flagging the clinical record.
- Remind your team member that they should not access the clinical record of their relative or friend unless they need to do so as part of providing care to them. Depending on the closeness of the relationship, this may mean stepping out of MDT meetings or team discussions.
- Consider the need to remind the person under our care that their information will not be shared without their permission and that their clinical record remains confidential to the team providing care. Offer them a copy of the information leaflet 'Privacy and your Information'.

3. What do I need to do if a member of my team is referred to StCH?

In this situation, as a manager, you will almost certainly already be having ongoing discussions with the team member about the person's fitness to continue to work or volunteer, involving the HR or Volunteering teams and following the appropriate procedures.

If the team member has actually been referred for care or support, you need to assure them that their confidentiality as a patient and their confidentiality as an employee or volunteer will be protected and that we have procedures in place to audit whether people are accessing records inappropriately. You may like to give them a copy of our leaflet 'Privacy and your Information'

Consider reminding them, however, that we also have obligations as an employer - to them and others - and explaining that the information that they have been referred may need to be shared in order to provide the best support to them or to other team members. Explain that information shared will be the minimum necessary.

You may like to consider and, if necessary, discuss the following:

- Would they like you to give the relevant clinical team the 'heads-up' that the referral is coming so that it can be handled sensitively?
- Explain that the information that they have become a patient may be added to their HR / record so that we can ensure that they have the support they need. This may include a referral to occupational health. If this is the case explain that their StCH clinical record will only be shared with the occupational health service with their permission.
- Do they want anyone else to know (e.g. work colleagues or friends from their own or other teams, senior members of staff) about their referral? If so, would they like your help in informing people or not?
- Are there any people who they would *not* want to know they have been referred? This can be difficult if these people are clinical and might be involved in providing care. Try to avoid making promises that can't be kept and if in doubt, speak to the Caldicott Guardian.

Please note that all referred patients are sent a letter asking about their preferences for receiving fundraising information. There is therefore NO need for you as a manager to inform the fundraising team and /or ask them to refrain from making contact if you think your team member may be registered on our supporter database.

If you are a clinical manager and the colleague who you manage is being referred to your *own* team, consider the following:

- whether it is appropriate for you / your team to see them clinically or whether you should ask a colleague or someone from another team to asses them instead if possible.
- Also consider whether, as a courtesy, they should be seen initially by a senior member of staff. However, try to avoid a situation whereby only one member of staff is involved in providing care or knows about the referral as this can cause difficulties with team working or out of hours.

See question 4 for more information and if you are unsure how to proceed, please discuss with your manager or the Caldicott Guardian.

Supporting and informing your team

4. I am a clinical manager and an employee, ex-employee, volunteer or supporter of St Catherine's has come under the care of my team. What do I need to consider?

As part of a holistic assessment, it is always important to discuss and document people's information-sharing preferences. You need to ensure that somebody in your team has done this or, if not, you need to do it yourself. You should also remember that friends and colleagues of this person may hear about their illness through social contacts and social media and be concerned about them and may want to ask questions. Remember also that some people who do not have a background in healthcare and who have had a long connection with the hospice may not understand rules about clinical confidentiality. They might even think that senior members of the hospice team will be told about their illness as a matter of course; it is important to explain that this is not the case.

You need to ensure that you or a member of your team explains to the person that information will not be shared without their permission and that their clinical record remains confidential to the team providing care. Offer them a copy of the information leaflet 'Privacy and your Information'. Consider specifically asking if there is any information they would like shared with anyone connected with the hospice who asks about them. If you think they may expect a number of members of the hospice team to know they are now a patient, you should consider proactively asking them if they would like any key colleagues or hospice managers or trustees informed.

Generally it is probably better to try and avoid providing clinical care to someone you currently line-manage, but this may be unavoidable at times. Ask the person who has been referred for their preferences about this and if you are unsure how to proceed, please discuss with your manager or the Caldicott Guardian.

You need, as a manager, to consider whether your team members need any additional support when caring for a person known to them. See question on support for team members.

N.B. It is acceptable to tell the HR or Volunteering team that colleagues in your team need support because someone they know or work with has been referred or admitted or is likely to die soon. However there is no need to share any personal or clinical details about the person receiving care with people within the HR or volunteering teams. They will not ask for this information.

5. What do I do if I find out that a former StCH colleague or volunteer who used to work with my team has been referred to or is under the care of StCH?

If you know and are in direct contact with the person or they have told you themselves you should consider explaining to the person that the clinical team will not be sharing any information with you. You might also like to reassure them that you will not share personal information about them with anyone at the hospice unless they ask you to.

You should consider the following and if appropriate, ask the individual:

- Does the individual want you to make any contact with the clinical team or anyone else at the hospice on their behalf? If they do, then liaise with the relevant manager. If you are unsure how to proceed, talk to the Caldicott Guardian.

- Do your - or other - team members need to know about the person's referral *in order to do their job* and does the person want you to inform anyone else at the hospice? If the person wants you to tell their former colleagues, or you feel that there are certain people who need to be informed in order to do their job, you can do so, but you need to consider whether you need to share their name or any clinical details. If you are in any doubt about how to proceed (e.g. you think someone should know a person has been referred but the person has asked you not to share information), DO NOT share any information without seeking advice from the Caldicott Guardian.

It can be difficult if this ex-colleague is now a member of your social circle and you hear about their illness informally or indirectly. Some people are happy to share a lot of information about their health socially; others are very private. Even if the person is open about their health with friends and their illness is widely discussed outside the hospice, or even discussed on social media, you are also an employee of StCH and have a duty to keep patients' records and heath information secure; this includes the fact that someone is under our care.

Depending on how well you know the person, you may like to consider contacting them, explaining that you heard from a social contact that they were unwell and asking the person how they want you to deal with enquiries from social contacts or people at the hospice who may be concerned about them. Unless the person has given you permission to discuss their illness with social contacts or colleagues, if you are asked for information directly or via social media it is best to respond that as an employee of the hospice you are not able to discuss whether people are under our care or to share any details. You can get further advice on individual situations from the Caldicott Guardian.

You must also consider whether your team members are likely to have to deal with social enquiries about the person. If they might, remind them that unless the person has directly given them permission to discuss their illness with social contacts or colleagues, they should respond that as a hospice employee or volunteer they cannot discuss whether people are under our care or share any details or post on social media without permission. Remind them that they can get further advice on individual situations from the Caldicott Guardian.

If you have been told about this person because people in your team may need support, you need to consider what support is appropriate. See Q7 and Q12.

6. What can I tell members of my team about the fact that a colleague or former colleague has been referred or is under the care of the hospice?

This depends on:
1) Whether your team members need to know this information in order to do their job and
2) What the person has said about who we can share information with.

If your team members need to know the person has been referred *in order to do their job* you should inform them promptly. Sometimes it can be hard to decide whether someone *needs to know* something in order to do their job and this needs to be considered on a case by case basis. The needs and wishes of the person under our care are paramount. The Caldicott Guardian is here to help you make these difficult decisions and is ultimately responsible for advising on whether something can be shared. Therefore, if you are in any doubt about whether you should share information, you should NOT share it until you know the person has given permission or until you have sought advice from the Caldicott Guardian about how to proceed.

If the person has said they are happy for information to be shared or has asked for people to be told, you should share the information promptly and sensitively, considering whether this is best done face to face or by other routes.

7. Someone well known to a number of hospice staff and / or volunteers is due to be admitted and I'm worried that colleagues might be upset; what can I do?

You should consider informing the managers of the colleagues who may need support about the admission so that they can put appropriate support in place. You may need to liaise with the HR team or Volunteering team about this. However, you should avoid sharing the name of the person being admitted or any clinical details unless you know that they have given permission for information to be shared. If you have any queries about what you can or should share, seek advice from the Caldicott Guardian. For further details about how to support staff and volunteers see Q12.

8. Someone known to a number of hospice staff and / or volunteers is a patient on the IPU. How should I respond to team members or volunteers asking about this person or asking to visit them?

You may like to consider reminding your team that this person will be cared for in the same way as all other people we support and that their confidentiality must be respected as we would for anyone else. Team members should be reminded that we do not share information with anyone outside of the team providing care without permission.

You should consider reminding your team that the person may be getting a lot of visits because it is so easy for people working or volunteering on site to just 'pop down' to the IPU. Consider reminding them that whilst many people will be happy to have a large number of visitors, for some people this is very tiring or embarrassing and may intrude on time spent with their close family and friends. Any member of staff or volunteer wanting to visit a patient on the IPU should check first with the nursing team, regardless of their role and how well they know the patient. The IPU nursing team will also try to establish whether the person or their family want any help with limiting visitors and will challenge people who are visiting without first checking with them.

9. Staff or volunteers are asking questions about how someone is or are upset that they 'aren't being kept updated' about someone's condition or. What should I do?

Remind them that we only share information about patients' health with those who *need* this information in order to do their jobs. It may be appropriate to enquire sensitively about why this staff member or volunteer feels they *need* or have a right to know this information. Asking might uncover anxiety or distress about what they might encounter. This may mean they need additional support or permission to step aside from caring from the person (if this is practical.) It may also be that other people might be putting pressure on them to divulge information. If other people are putting pressure on them to divulge information, help them respond to this and explain that they ought to feel proud to work for an organisation that takes its legal obligations about confidentiality seriously.

If the staff member or volunteer knows the patient and their family socially / outside work, you can consider suggesting that they ask a member of the family for an update. However, if you are aware that the person has a wide social circle of people who work or volunteer at the hospice, then you may consider alerting a member of the clinical team that there may be a number of enquiries. They can liaise with the person or the family and ask them whether they need any help in responding to queries from colleagues and former colleagues.

10. A person well known to a number of StCH former employees, supporters, or trustees is on the IPU. Do we need to do anything different?

Not really; this person should be cared for and their confidentiality respected as we would for anyone else. They should be asked about their information-sharing preferences and reminded that we do not share information with anyone outside of the team providing care without permission. A member of the clinical team should consider specifically acknowledging to the person that they might get an unusually large number of visitors or people asking after them because of their connection to the hospice. Consider asking if they or their family need any help in managing this. It can sometimes be difficult for people under our care or their families to discourage visitors themselves. If they are struggling with this we can help 'filter' by having a message at reception and asking people to speak first to the nursing team.

As a manager, you should also be aware that your team members may be having to deal with a number of enquiries from people about this individual and can be put under pressure to divulge information. Occasionally, people with a connection to the hospice might think that because they know many members of the team, they do not have to abide by normal conventions like asking nursing staff before visiting and they might ask inappropriate questions. You should consider reminding your team members that they need to challenge this inappropriate behaviour and you should ensure that you are available to support them in doing this if needed. This can be difficult as often the person behaving inappropriately means well and has little insight into their behaviour.

11. A member of staff or volunteer in my team has unexpectedly encountered an acquaintance of theirs at the hospice. They didn't know this person was under our care or had a relative under our care. What do I need to do?

This happens relatively frequently and can cause embarrassment on both sides. You need to talk to your team member and see whether their connection to this person makes it hard for them to fulfil their role. You also need to see whether they need any additional support.

Consider also the need to remind your team member of their obligations about confidentiality. They need to keep the fact that they have encountered this individual confidential and should not share any information with social contacts. Remind them that as a hospice employee or volunteer they cannot discuss whether people are under our care or share any details without permission. Remind them that they can get further advice on individual situations from the Caldicott Guardian. If necessary, give them guidance on how to respond tactfully but appropriately to questions from social contacts and remind them not to post on social media.

If appropriate, you may like to suggest that they approach the individual and assure them that they will not disclose the fact that they have encountered them at the hospice unless they are asked to do so. Alternatively you may consider it more appropriate to approach the patient or family member yourself (or ask a clinical colleague to do so). You should reassure them that nothing about them will be shared with people who are not part of the team providing care unless they give permission.

12. A member of my team or colleague who used to work with my team has died. Can I share this information with my team or the wider hospice team? And can I say where they died or what from?

Yes, you can tell your team that someone they used to work with has died. The fact that someone has died is a matter of public record, so can be shared, and if the person is still a member of your team it is important that colleagues are informed in a sensitive and timely way.

However, you need to consider the following:

- Whether and when the family want this information shared. Some bereaved families will want to tell people themselves where possible; others will be grateful if we offer to help them share the news within the hospice community.

- Which colleagues need to know and the timing of telling them. Some team members might need to know very soon after the death (e.g. because the person has died on the IPU and they are on shift that day). In this case, please remind them not to make any public comments or share the information (including posts on social media) before the person's immediate family may have had a chance to inform extended family and friends.

Your role *as a manager* is to consider who needs to know about the death in order to do their job. Consider if there are key colleagues outside your team (e.g., people who worked closely with the person or were friendly with them, senior colleagues or managers) who might need to know promptly about the death in order to support people in their teams. If this is the case then you need to liaise with these peoples' managers (or with the HR department if, after discussion with the family or others, you think that the whole hospice team should be informed.) Consider the best means of informing people (face to face, email, telephone etc) and seek advice if you are unsure. Remember that the Caldicott Guardian is here to help make decisions about what can be shared - so seek advice if you are in any doubt. If you think there is a reason to inform trustees that someone has died under our care, please liaise with the Chief Executive.

Consider whether you *need* to mention place of death and *avoid* mentioning cause of death if the person died under the care of St Catherine's, unless you know that the person was happy for this information to be shared. Although date, cause and place of death is a matter

of public record and can be found out from death registration records, it does not become a matter of public record until the death is registered. St Catherine's Hospice has a common law duty of confidentiality to its patients and we should try to protect sensitive data like whether someone died under our care or what illness they had where practicable.

If you need any advice on what you can share and how please ask the Caldicott Guardian or Deputy.

13. How can I support staff and volunteers in my team when they are caring for someone they know or when someone they know has died?

You need to consider whether anyone in your team will need additional support. Remember that each individual is different and will have different coping strategies so whilst you can remind the whole team that support is available it is better to talk to people alone about their individual needs. There are a range of different ways to help. You can refer to the Wellbeing Resources on the Intranet and discuss with the HR or Volunteering team for more details.

Funerals and other arrangements

14. How can staff or volunteers mark the death of a colleague?

There are a number of ways this can be done. However, first and foremost it is important to respect the wishes of the person who has died and of their family, particularly if arranging a public tribute. Remember that not everybody wants public tributes and not everyone is comfortable participating in them.

You may like to consider options such as:

- having a couple of minutes' silence at a team meeting,
- sending a letter or card or book of condolences to the person's family
- reminding people that the Quiet Room is available for quiet reflection
- asking the Spiritual Care Coordinator to conduct a short service.

Remember that people grieve differently and have different ways of marking the death of someone they know. Try to avoid giving the impression to your team members that participation in any tribute is compulsory.

We have on occasion gathered outside the hospice as a mark of respect when a staff member or retired staff member has died on the IPU and leaves the hospice for the last time. This sort of public hospice tribute is made at the discretion of the SMT and in liaison with the person's family. It is generally reserved for current members of staff or for people who made a significant contribution to the hospice over a number of years, *remained closely involved* and are known to a number of current employees.

Before considering sending flowers to a funeral or making charitable donations, check what the person's family want. Most families make this clear when they tell people about funeral arrangements.

15. Should I publicise details of the funeral arrangements within the hospice?

This depends on the wishes of the person's family. You should consider whether you or someone else from your team needs to liaise with the family about funeral arrangements to

check how they feel about representation from the hospice. If they have asked you to share details of the funeral with people at the hospice then of course you can do so as appropriate. Similarly if the family have publicised details in a newspaper or on social media then you can draw people's attention to this as appropriate. Depending on the family's wishes, you need to consider whether these details are shared with the whole hospice or just with close colleagues or friends of the person who has died.

16. Should I expect my team members to attend the funeral? What do I do if a number of colleagues want to attend?

If the family have said the funeral is open to work friends and colleagues then you need to balance the need to run your service or department with the need to let colleagues attend. Try to plan ahead as far as possible and discuss with your team members and managerial colleagues and /or the HR or volunteering teams if you think additional cover may be needed. Remember that it will not always be possible for everyone who wants to attend to do so and some people may prefer not to. Involve your team members in this decision. Consider whether those unable to attend may want to spend a short time in the Quiet Room at the time of the funeral.

17. Who can attend a funeral as an official representative of the hospice?

An official representative of the hospice in this context is usually the Chief Executive, a SMT member, a trustee, or the Volunteering Development Manager. There are times when it is appropriate for a departmental manager or member of the Volunteering team to fulfil this role instead, particularly if they had a closer connection with the person who has died.

18. Should I make the Order of Service available following the funeral?

This depends on the wishes of the person's family. Following the funeral, consider whether it is appropriate to display a copy of the Order of Service in a team office or in the Quiet Room for colleagues who were unable to attend.

19. Where else can I get advice and support about matters relating to confidentiality and what can be shared?

You may like to remind yourself of the Information Governance Policy and some of the legal frameworks within which we operate (e.g. the Data Protection Act and Access to Health Records Act.) Remember the 7 Caldicott Principles for the sharing of patient identifiable information. These are reproduced for convenience in below. If in any doubt remember that the Caldicott Guardian is here for advice and support.

You may also like to familiarise yourself with the content of our leaflet 'Privacy and your Information' and with the hospice Privacy Statement.

20. Where else can I get advice and support about matters related to support of colleagues and volunteers?

The Human Resources Management Policy and Volunteering Policy set out broad principles of St Catherine's Hospice approach to the support of employees and volunteers. You can

get advice (both general and related to the support of particular individuals) from a member of the HR team or the Volunteering Team. You may also like to refer to the Wellbeing Resources on the Intranet.

The **Caldicott Principles** for the Sharing of Patient Identifiable Information

1. **Justify the purpose(s)**
   Every single proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use patient identifiable information unless it is necessary**
   Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. **Use the minimum necessary patient-identifiable information**
   Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
4. **Access to patient identifiable information should be on a strict need-to-know basis**
   Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.
5. **Everyone with access to patient identifiable information should be aware of their responsibilities**
   Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
6. **Understand and comply with the law**
   Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.
7. **The duty to share information can be as important as the duty to protect patient confidentiality**
   Professionals should in the patient's interest share information within this framework. Official policies should support them doing so.