ST CATHERINE'S HOSPICE

Data Protection Policy

Document Control Table

Document Title:	Data Protection Policy
Document Ref:	POL 53
Author (name and job title):	Karen Anderson, Head of HR
SMT sponsor:	Eric Norman, Director of Finance and Site Services & SIRO
Members of stakeholder group:	IG Group
Target audience: - all staff & volunteers - staff only - clinical staff only - other (please specify)	All Staff and Volunteers Contractors Consultants Agency Workers Students
Key words:	DPA, Personal Data
Version Number:	1
Document Status:	Approved
Ratified by:	Information Governance Group
Date Approved:	12 July 2016
Effective Date:	19 July 2016
Date of Next Review:	Sept 2019

Amendment History

Version	Date	Author	Notes on revisions (inc reason)
CO-12	June 2010	Richard Tullet	Complete review

Associated Documents

Contract of Employment and Confidentiality Code of Conduct
IT Security Policy
Mobile Device Policy
Media Policy
Social Media Policy
Information Governance Policy
Consent Policy
Adult and Child Safeguarding Policies
Incident Management Policy
Raising a Serious Concern Policy
HR Policy and supporting policies
Records Management Policy
CCTV Policy
Volunteers Policy

References

Data Protection Act 1998
Freedom of Information Act 2000
Data Protection (Processing of Sensitive Personal Data) Order 2000
Computer Misuse Act 1990
Human Rights Act 1998
Health & Social Care Act 2008
Common Law Duty of Confidence
Access to Health Records Act 1990
Caldicott Principles

To ensure you are using the current version of this policy, please access it directly via StCH intranet; other versions cannot be guaranteed as current

Contents

1. Introduction

The policy sets out in broad terms the duties placed upon St Catherine's Hospice by the common law duty of confidence, the Data Protection Act 1998 (DPA) and guidance provided by the Information Commissioners Office, and other relevant bodies.

Penalties could be imposed on the Hospice and/or on staff for non compliance with relevant legislation. Therefore this policy applies to all staff, anyone working on behalf of the Hospice (e.g. consultants, contractors, agency workers), volunteers and students.

The DPA is closely linked with the Human Rights Act and the Freedom of Information Act. The focus of the DPA is on promoting the rights of living individuals in respect of their privacy and the right to security and confidentiality of their data. It applies to all person identifiable data, whether held manually or electronically. The responsibility to maintain confidentiality of that data resides with the Hospice, even if an agent or subcontractor processes that data.

The DPA does not guarantee personal data privacy at all costs, but aims to strike a balance between rights of individuals and the sometimes competing interests of those with legitimate reasons for using person identifiable data.

The DPA allows people to find out what information is held about them by making a Subject Access Request.

The Hospice is obliged by law to register all process activities with the Information Commissioners Office on a annual basis and failure to comply with this requirement is a criminal offence. The renewal date is November each year.

2. Purpose

Data protection is a large and complex issue which affects the whole organisation and should be understood by every member of staff, not just one delegated person. This policy sets out how the Hospice aims to meet its legal obligations concerning the security and confidentiality of person identifiable data**.**

3. Scope of policy

For the purpose of this policy "staff" is used as a convenience to refer to all staff regardless of occupation, including but not restricted to permanent, fixed-term, contractors, bank, agency, temporary, those on honorary contracts, visiting students and volunteers.

This policy relates to all person identifiable data held by the Hospice, both clinical and non clinical, that are received, stored, transmitted or communicated both within and outside of the Hospice.

Person identifiable information may be in any form including, but not restricted to, the following:

- paper records or documents
- telephone conversations (inc voice recorded information)
- e-mails and attachments
- computers and other storage devices (including CDs, memory sticks or other portable devices/media, fax messages)
- Close Circuit Television (CCTV)

4. Definitions

In this policy, certain terms are used which have the following meanings:

Data Controller: means an organisation which processes personal data, and is registered to do so with the Information Commissioner, by the Data Protection Officer. St Catherine's is a 'data controller' for the purposes of the Data Protection Act 1998.

Personal data: any information, held in any format relating to a living individual who can be identified either from the data or from the data in conjunction with other information that is in, or likely to come into, the possession of the data controller. This includes employment details, patient and client information, donor information, and information captured on CCTV.

Sensitive personal data: means information relating to any of the following:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other similar beliefs
- Memberships (including of a trade union)
- Physical or mental health or condition
- Sexual life and orientation
- Criminal or civil offences or alleged commission of any offences or any proceedings for any offence committed or alleged to have been committed
- Personal life

Data subject: means the person who is the subject of the personal data.

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

5. Policy statement & aims

The purpose of this policy is to ensure staff, volunteers, contractors, consultants and students understand their responsibilities in terms of the DPA and confidentiality, and are confident in the processing of personal data.

The following information is a summary of legislation relevant to the protection and use of person identifiable information. All staff should be aware of their responsibilities under these Acts and have due regard for the law when collecting, using or disclosing personal confidential information.

5.1 Data Protection Act 1998

The Data Protection Act (DPA) is based on the EC Data Protection Directive 95/46/EC which seeks to 'further protect individuals by controlling the collection, use, storage and movement of personal data'. In general terms, it gives individuals the right:

• of privacy
• to know the purposes for which their data is being held and processed
• to know who their data may be disclosed to
• of access to their data
• to prevent the use of their data in certain circumstances

The DPA places legal obligations on everyone who processes personal data. There are eight Data Protection Principles that must be complied with to ensure the data is held and used in accordance with the DPA. The eight Principles to processing personal data are:

1) Data must be obtained and processed fairly and lawfully.
2) Data can only be collected and used for specified purposes and shall not be further processed in a manner incompatible with that purpose(s).
3) Data must be adequate, relevant and not excessive in relation to those purposes.

4) Data must be accurate and kept up-to-date.
5) Data must not be kept for longer than is necessary for that purpose.
6) Data shall be processed in accordance with the rights of the data subject.
7) Data must be kept safe from unauthorised access, accidental loss or damage
8) Data shall not be transferred to countries outside the European Community unless the country being transferred to has adequate protection for the rights and freedoms of data subjects in relation to processing of personal data.

With effect from April 2010 (introduced by the Criminal Justice and Immigration Act 2008), there are a revised number of criminal offences under the DPA that the Hospice and individual employees can be prosecuted under:

- Processing person identifiable data without notifying the Information Commissioner
- Processing person identifiable data for any purpose other than that covered by the Hospice's Notification
- Un-authorised disclosure of person identifiable data e.g. disclosure to a person or organisation not entitled to receive it.
- Failure to comply with an Information/Enforcement notice issued by the Information Commissioner.
- Modifying personal data subject to a 'Subject Access Request'
- Breaches of Section 55 of the DPA (this is knowingly or recklessly disclosing information).

The Data Protection (Processing of Sensitive Personal Data) Order 2000 sets out additional circumstances where sensitive person identifiable data may be processed. For example, in the prevention or detection of any unlawful act if "in the substantial public interest". It must only be processed when one of the following conditions has been satisfied:

- Data subject has given explicit consent
- It is required by law for employment purposes
- It is needed in order to protect vital interest of the individual or another person
- It is needed in connection with the administration of justice or legal proceedings

The retention of Hospice records and data covered by the DPA will comply with the Charities Act 2011 and Companies Act 2006, Health and Social Care Act 2008, however where appropriate guidance from other professional bodies will also be taken into account (eg NMC, BMA and CQC).

Handling of credit and debit cardholder data will be in line with the Payment Card Industry Data Security Standards.

6. Accountability and responsibility

Chief Executive is responsible for:
- ensuring adequate resources are in place to ensure the implementation of this policy and delegate day to day responsibility for this to Data Protection Officer, SIRO and/ or Caldicott Guardian.

Data Protection Officer (DPO) is responsible for:
- ensuring review and implementation of this policy, the promotion of data protection compliance and best practice in an organisation
- providing advice and guidance in the use and sharing of personal information (with special regard to staff and volunteers information)
- ensuring that all staff have read and signed the StCH Confidentiality Code of Conduct
- overseeing data subject requests for staff and volunteers information.

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

SIRO is responsible for:
- ensuring the organisation's information risk is identified and managed, and that appropriate assurance mechanisms exist.

Information Governance Lead/Quality & Information Manager is responsible for:
- monitoring actual or potential reported (via Datix) information security incidents within the organisation
- ensuring effectiveness of IG incident reporting system and procedures.

Information Asset Owners are responsible for:
- managing/maintaining security and integrity of the information assets assigned to them.

Senior Managers and 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 personal information security, confidentiality and records management
- ensuring their staff undertake compulsory information governance & DPA training
- the security of the physical environment where their team operates and where information is processed and stored.
- ensuring that all sources of person identifiable information sent into or out of the Hospice are advised of the requirements of this policy.
- reporting and investigating any breaches of this policy through the Datix Incident Management system

ICT Manager is responsible for ensuring all computer hardware and software is safeguarded in line with the DPA and provide relevant reports to the appropriate person (SIRO, DPO, Caldicott Guardian) to assist with monitoring compliance or incident investigations.

All staff 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
- reporting any breaches of this policy through the Datix Incident Management system
- checking that personal data held on themselves is accurate and up to date, and updating HR database or the HR Team accordingly of any changes (e.g. change of address).

Information Governance Group is responsible for:
- overseeing day-to-day information governance issues
- 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.

7. Procedure/Processing data

All staff, or other persons who act on behalf of the Hospice, must process data in line with this policy, local procedures and retention of data procedures set out in the StCH Records Management Policy, and with the appropriate consent of the individual that the information relates to.

7.1 Requests for information

Requests for access to information held by the Hospice (subject access requests) may be made in line with the DPA and the StCH Subject Access Request Procedure (see StCH Records Management Policy).

The Freedom of Information Act 2000 give members of the public the right to request information from a public body which may not otherwise be accessible via approved public documents such as Annual Reports etc. While this does not apply to non public bodies such as the Hospice, all reasonable written request for information will be considered, provided that they would not breach this or other related policies.

7. 2 Retention of Records

Principle 5 of the DPA states that data should not be kept for any longer that necessary, and therefore data should be managed in line with local procedures as set out in the StCH Records Management Policy.

8. Dissemination

This policy will be circulated to all staff via email by the author when it is first issued and when it is updated. Managers must ensure that all their staff are aware of the policy and where to find it through, for example, team meetings and 1:1s. Information will also be disseminated in the Headlines and through staff updates.

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

Policy can be accessed via the intranet.

9. Monitoring and review

This Policy will be reviewed every three years

All staff are responsible for monitoring their personal compliance with guidance detailed in this policy. Any breaches or near misses must be reported immediately via the Datix system and to the line manager. Where applicable, the Serious Untoward Incident Policy may be invoked. Breaches must also be reported to the SIRO, Data Protection Officer and/or the Caldicott Guardian.

Monitoring of this Policy will be informed by the IG complaints and IG incidents reported and regular reports will go to the IG Committee, in addition to regular review of DPA compliance and IG incident trends.

Appendix 1

Processing personal and sensitive data

We process personal information to enable us to provide health services to our patients, and other service users, to maintain our accounts and records, maintain and promote our services, comply with health and safety and other statutory obligations, and to support and manage our employees and volunteers.

Who information is process about

- patients and other service users
- customers and clients
- staff, contractors, consultants, agency workers
- suppliers
- business contacts
- professional advisers
- volunteers
- donors

This information may include (dependant on the who):

- Personal details - eg: address, date of birth
- family details
- lifestyle and social circumstances
- finance details
- employment and education details/history

The processing of sensitive classes of information that may include:

- physical or mental health or conditions
- racial or ethnic origin
- trade union membership
- religious or other beliefs of a similar nature
- convictions, proceedings and criminal acts

Where necessary or required to do so we share information with:

- healthcare professionals
- social and welfare organisations
- family, associates and representatives of the person whose personal data we are processing
- Government agencies
- financial organisations
- current, past and prospective employers

Policy Impact Assessment

The impact assessment is used to ensure:

- 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 any new policies or revisions to existing 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 origins - nationality - gender - culture - religion or belief - sexual orientation (including lesbian, gay & bisexual people) - age - disability (eg physical, sensory or learning) - mental health	**No**	
b.	If potential discrimination has been highlighted, are any exceptions valid, legal and/or justifiable?	**NA**	
c.	Is the impact of the policy likely to be negative? If so, can the impact be avoided or reduced?	**NA**	
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	**No**	
b.	If so, have these issues already been raised with the Information Governance Group? What action has been agreed?		

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

Caldicott Guardian (StCH Medical Director)

Data Protection Officer (StCH Head of Human Resources)

Senior Information Risk Owner (StCH Finance & Site Services Director)

Quality & Information Manager

Services Information Coordinator