serving the local community

St Nicholas Hospice Care

A Registered Charity No. 287773

Data Management Policy

Originator: **Barbara Gale**
Chief Executive

Review date: **May 2013**

Revision date: **May 2015**

Approved by: **Clinical Committee**

Date of Meeting: **5 September 2013**

Name of Chairman: **Sue Hayter**

Approved by: **Board of Trustees**

Date of meeting: **17 October 2013**

Name of Chairman: **Adrian Williams**

Contents

1. Policy statement

St Nicholas Hospice Care (SNHC) is required to maintain a wide variety of records and information. SNHC is committed to ensuring that information, in whatever its context, is handled as set out by prevailing law, statute and best practice.

SNHC places significant importance on protecting personal data, yet recognise that it is imperative it shares personal information to support its service delivery functions.

SNHC recognises its responsibility to ensure that all records, including health records and databases, are managed appropriately. Staff will ensure that:

- People are informed appropriately about the reason the data is held and that data is used only for those purposes
- The data held must be adequate, relevant and not excessive
- The data is accurate and procedures are in place to monitor this
- The data is held only as long as required and then archived or destroyed
- Data is protected from unauthorised access or loss
- All data (including archived data) must be able to be recalled and printed easily

It is essential that employees of SNHC co-operate with this policy so as to safeguard against a breach of the Law. There is a need to ensure the provision of appropriate management of the data and to protect the data.

2. Introduction

St Nicholas Hospice Care is an independent charity delivering specialist palliative care to patients and their families within the communities of West Suffolk and Thetford. Care is delivered by a specially trained multidisciplinary team supported by a large team of volunteers to patients within our Sylvan Ward, Community Hospice Team, Orchard and Burton Centres. The organisation also includes an Education Department that delivers palliative care education to the local community, a Fundraising Department that manages a range of fundraising activities and a Retail Section with several shops in the local community staffed by paid staff and volunteers.

This policy relates to any data including that which is held manually and electronically. SNHC recognises the importance of handling data in a way which respects the individual or organisation concerned and complies with legislation and best practice.

2.1 Definitions

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

Application – means an application in writing:

- By the patient
- By a person authorised in writing (see Appendix 3) to make the application on the patient's behalf
- Where the record is held in England and Wales and the patient is a child, a person having parental responsibility of the patient
- Where the record is held in Scotland the patient is a pupil, a parent or guardian of the patient
- Where the patient is incapable of managing his or her own affairs, or where the patient has died, the patient's personal representative and any person who may have a claim arising out of the patients death – see Sections 5, 6,and 7 of this document

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

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

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

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

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

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

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

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

Health professional – as defined in the Data Protection Act 1998, means any of the following:

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

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

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

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

- From those data
- From those data and other information in the possession of, or likely to come into the possession of the Data Controller

Personal Data includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Personal Data
may also include opinions expressed by the data subject – additional guidance can be found in the Information Commissioners office document 'Data Protection Technical Guidance Determining what is personal data' v1.0 21.08.07
http://www.ico.gov.uk/upload/documents/library/data_protection/detailedspecialist_guides/personal_data_flowchart_v1_with_preface001.pdf

Processing – means

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

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

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

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

Staff – this encompasses staff, volunteers, sessional workers and those on placement.

3. Responsibilities and Accountability

Failure to comply with any aspect of this policy could create a breach of statute for which the organisation could be held liable. Such an issue could lead to disciplinary action being taken under SNHC's disciplinary procedure.

Chief Executive Officer (CEO)

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

Information Governance Lead

The Information Governance Lead is responsible for ensuring the Hospice's compliance with Information Governance requirements. Key responsibilities include:

- Ensuring that there is an up to date IG policy in place;
- Ensuring that the Hospice's approach to information handling is communicated to all staff, volunteers and contractors, and made available to the public;
- Coordinating the activities of staff given data protection, confidentiality and Freedom of Information responsibilities;
- Monitoring the Hospice's information handling activities to ensure compliance with law and guidance;
- Ensuring that staff and volunteers are sufficiently trained to support their role;
- Ensuring that the Hospice submits its annual IG Toolkit Assessment;
- Supporting monitoring visits from the commissioning organisation.

Information Governance Lead responsibility has been assigned to the Director of Finance.

Directors

Directors take responsibility for their departments in:

- Maintaining relevant registrations
- Managing databases

- Facilitating training sessions
- Dealing with access requests
- Acting as initial point of contact for any data protection issues which may arise within their Department

Managers

Managers are responsible for the day to day management of information and for the training of staff who use and have access to information.

Staff

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

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

4. Procedures and Implementation

4.1 Data Protection

In accordance with the Data Protection Act 1998, the use of data must follow the Eight Data Protection Principles:

1. Personal data shall be processed fairly
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Following the Data Protection Act it shall be the duty of a Data Controllers to comply with the data protection principles in relation to all personal data with respect to which he or she is the data controller. The data controllers for St Nicholas Hospice Care are the Chief Executive Officer and the Directorate Team, which consists of the Clinical, Fundraising, Finance and Personnel Directors.

4.2 Security and Confidentiality

All information relating to identifiable individuals and any information that may be deemed

sensitive, must be kept secure at all times. SNHC staff will adhere to procedures that protect against unauthorised processing of information and against accidental loss, destruction and damage to this information. (See Appendix 1).

4.3 Records

In line with the Data Protection Act people will be informed about the purpose of hospice records and how the information may be shared, if at all. Paper and electronic data is held by SNHC in relation to patient and family care, personnel and volunteer data, fundraising supporter and donor data.

4.3.1 Healthcare records

Health records are held on paper and electronically and any member of clinical staff can contribute to the records and can write in any part of the notes as long as they are competent to have either assessed, planned, delivered or evaluated care.
(See Appendix 2 for guidance)

Important issues communicated with patients or carers must also be recorded. Qualified professionals will be responsible for supervising the notes written by volunteers and students and determining whether they need a counter signature. Nursing Assistants do not need their entries countersigned.

What is written in the records must, whenever possible, be constructed with the involvement of the patient/client or their carer. This is particularly pertinent to the issues of consent and "Thinking Ahead" recording. Their feedback/comments regarding the assessment, treatment and care plan must be noted. (Patients must be informed of the uses to which information about them and any record of treatment may be put, together with any intended disclosure to outside agencies or persons as per consent guidelines.) Staff have both a professional and a legal duty of care. Their record keeping must therefore be able to demonstrate:

- A full account of their assessment and the care that has been planned and provided
- Relevant information about the condition of the patient/ client at any given time
- The measures taken by staff to respond to needs
- Evidence that staff have understood and honoured their duty of care, that all reasonable steps have been taken to care for the patient/client and that any actions or omissions have not compromised the patients safety in any way
- A record of any arrangements that have been made for the continuing care of a patient/client.
- Weighing of risks and benefits.
- Rationales for interventions.

When not being used for patient care, all health records must be kept in a secure location, away from observation by the public, with access limited to staff working in the Clinical Department.

Counselling Records - Counselling may be undertaken by members of the Family Support team or by qualified sessional workers, seeing patients or relatives on behalf of Family Support. Records will be made in the main Health Care Record notes or in the Carer Records when there is no multidisciplinary team involvement. The Family Support administrator will facilitate this process for sessional workers.

Any working notes or impressions of a counselling session, which may serve as an aide memoir to subsequent sessions for example, will be retained for 12 months before being

destroyed; during the period in which such records are kept, they will be subject to client access under the Data Protection Act (1998) provisions and will be available within the Family Support filing system.

Nicky's Way - Records for the children's bereavement service may be made for assessment, preparation or follow-up purposes with regard to individual children and families, and kept securely in the Family Support Team filing system. These records are subject to the same data protection and access provisions as all other hospice records.

Research, teaching and supervision - Patient/client records may be used for research, teaching purposes, audit and clinical supervision. The principles of access and confidentiality are paramount and the right of the patient/client to refuse access to their records must be respected. The local research ethics committee must approve the use of patient/client records in research.

4.3.2 Photographs and videos

Consent is always obtained from individuals who have been photographed or recorded for Hospice communication purposes. The form clearly states what the information may be used for and asks the participant to state if they wish the image or broadcast to be used for one occasion only or in perpetuity. There is a specific form for under 16s.

Photographs/ video/audio recordings are stored electronically on the Marketing's central drive, which only is accessible by staff members with permission and the consent forms are stored in paper format in the Marketing office.

On the advice of the Information Commissioners Office (ICO), all archived photographs (i.e. pre May 2008) are used only when the individual cannot be identified. For example as a group shot or with a general image that doesn't carry a caption.

See Appendix 6 and Appendix 7 for the consent forms.

4.3.3 Personnel and volunteer data

Personnel records are defined as information about people employees or volunteers or contractors or temps), created or received in the course of business, and captured in a readable form in any medium, providing evidence of the functions, activities and transactions of those people. These may be held in the Personnel and or Finance Department (when relating to payroll matters) or by the person's line manager.

4.3.4 Fundraising data

Fundraising records are defined as information about people created or received in the course of fundraising and captured in a readable form in any medium, providing evidence of the functions, activities and transactions of those people. These may be held in the Fundraising Department or on the Fundraising database.

4.4 Informing people on the use of their Information

The Data Protection Act 1998 states that individuals have to be provided with information where organisations or person(s) hold and use their personal information, the information to be provided must include:

- The purposes for which it is being used

- The likely disclosures of their information
- The likely consequences of the processing
- Any other information that is necessary

Posters should be displayed in public areas and leaflets made available to further complement this requirement. For information collected via the St Nicholas Hospice Website a Privacy Statement will be available.

Providing advice and responding to individuals about the use of their information
There may be occasions where SNHC is considering using an individual's personal information for another purpose or disclosing it to a person or organisation that the individual(s) would not have anticipated. In which case, SNHC may need to make arrangements to inform individuals about these new uses of their data.

People may also contact SNHC about a number of issues related to use of their personal information, this may include:

- Objections to how their personal information is processed
- Requests for certain possible disclosures of their information to be restricted
- Requests for detailed information about how their information is used by SNHC

Giving people the opportunity to opt out of receiving information sent out by SNHC
Requests from people to withdraw their name from a distribution or marketing list will be dealt with within 28 days.

4.5 Individual rights

An individual is entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person). Neither are they entitled to information simply because they may be interested in it. An individual's rights include:

- A right of access to a copy of the information comprised in their personal data
- A right to object to processing that is likely to cause or is causing damage or distress
- A right to prevent processing for direct marketing
- A right to object to decisions being taken by automated means
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
- A right to claim compensation for damages caused by a breach of the Act.

4.6 Procedure to access personal data

1. A request for access to personal data must be received in writing (hard copy or electronic)
2. A response must be made within 40 calendar days
3. The request will be managed by the department director
4. The identity of the person making the request must be confirmed by them producing relevant identification (unless the person is personally known to a member of the organisation).
5. The department director must ensure the information is in intelligible form.

4.6.1 Access to health records

See Appendix 3 for procedure to access health records.

Formal and Informal access to health records – access to health records has always occurred on a voluntary and informal basis between clinician and patient. Whenever

possible, access should be given in this way whilst a patient is undergoing treatment or care. It only applies to particular episodes of care to which the applicant actually refers and is not an opportunity for the applicant to peruse the complete medical notes.

Recognising and responding to a subject access request
Access encompasses:

- The right to obtain a copy of the record in permanent form, and
- The right to view a record without obtaining a copy - NB this is discretionary in regard to medical records
- The right to have information explained where necessary, e.g. medical abbreviations

4.7 Information Sharing

All personal information that is used in the protocol sharing arrangement must meet the conditions for processing as laid down in the Data Protection Act 1998. Where that personal information also has a duty of confidence and it is to be shared for a different purpose to that for which it was given, it should only be disclosed if one of the following requirements has been met:

- The individual has given their consent
- The disclosure is a requirement of a statute of law
- There is an overriding public interest in making the disclosure

At the start of any information gathering arrangement, procedures should ensure that an individual should be fully aware and in agreement that their personal information is to be shared for the purpose specified in that arrangement.

It must be appreciated, however, there may be occasions where confidentiality is not absolute and it could be essential that it be breached. This may be appropriate where it becomes necessary to protect an individual from harm such as in a child protection case; protection of vulnerable adults or personal information is required for a serious crime investigation. Also, a stature of law might allow a disclosure without consent for example – Public Health legislation stipulates that designated SNHC staff need to notify the relevant authority where a person is suspected of contracting a notifiable disease.

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

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

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

Where SNHC receives a request for personal information from the police, certain information can be released if a statute of law dictates the need for disclosure e.g. -

- The Police have produced a court order
- The information is required under the Road Traffic Act

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

4.7.1 Controlled Drugs

SNHC is part of an Information Sharing Protocol with Suffolk and Norfolk Constabulary Information Systems, to facilitate the sharing of concerns, suspicions and incidents in relation to Controlled Drugs. The Accountable Officer for SNHC is responsible for the sharing of any relevant information.

4.7.2 Sharing or selling fundraising data

SNHC will not sell or share information to third party organisations. SNHC does use third party organisations to manage or sort data as part of our fundraising activities, but the information gathered in this way remains the legal responsibility of SNHC and the data is treated with the same level of care as if SNHC were handling it directly.

4.8 Information technology

SNHC is committed to providing information resources to help staff work in an efficient manner. Staff are expected to use these resources responsibly and not to abuse the trust placed on them. Staff must conduct themselves honestly and respect copyright, licensing, property rights and the privacy of others. Guidance on appropriate usage is found in Appendix 5

Electronic communications facilities include:

- Website
- Electronic mail
- Social networking sites
- Internet usage
- Use of PCs, Laptops, PDAs
- Audio visual devices
- Telephone equipment including mobile phones, Dictaphones and voicemail
- Digital cameras (including mobile phone cameras)
- Any type of mobile data storage device (CDs, data sticks etc)

SNHC website will ensure that:

- Users must be able to opt out of any disclosure
- Users must be advised who will be using the information and who it may be disclosed to
- Users must be advised of Cookie usage
- A Privacy Policy is available

The principles for electronic record keeping are the same as for paper records. In addition, when using electronic documentation, there must be procedures to ensure:

- Physical security/equipment security
- Access control (at different levels, if necessary)
- User password management
- Computer virus control

- Data back-up
- Computer network management
- Data and software exchange
- Validation
- Adequate training for all users

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

4.8.1 Use of the Internet

Staff must not

1. Access illegal, pornographic, obscene, abusive (racially or sexual) Internet sites from work.
2. Use the Internet for private commercial, political or other non-work related purposes, or for making personal profit.
3. Use the Internet to download software or other programs without seeking prior approval of the Hospice's Finance Director. This is most important because of the potential risk of downloading malicious programs.
4. Use the Internet at work for personal Internet "chatting", messaging or for playing computer games.
5. Subscribe to any bulletin boards, newsgroups or any other Internet service of any kind without prior discussion with their line manager.
6. Download, copy or transmit to third parties the works of others without their permission as this may infringe copyright.
7. Use public social networking sites to discuss work related issues.

Usage of the Internet may be monitored without notice.

4.8.2 Mobile Computers

Laptops and smart devices such as tablets and phones offer portability, access to data when away from your desktop PC and are a useful tool for business use. Due to their portability certain security risks arise namely:

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

Therefore staff should:

- Ensure that laptops and smart devices are password protected
- Access sensitive or confidential information remotely and not save it onto the device's local storage.
- Ensure that the device is stored securely when not in use

4.9 CCTV

CCTV is used by SNHC. Live images can be accessed via the Internet and are designed to improve security of the building, specifically for Sylvan Ward staff and particularly out of hours when there is no receptionist on duty.

SNHC have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of staff, patients and families. It will not be used for other purposes. An annual review of the use of CCTV is conducted.

Signage is displayed notifying the public of the use of CCTV.

This CCTV system and the images produced by it are controlled by SNHC which is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998).

In line with the CCTV code of practice SNHC will:

- Notify the Information Commissioner annually
- Allocate the Finance Director to be responsible for the operation of the system
- Ensure the system can provide clear images to be used if required
- Ensure the cameras are positioned only to record those visiting the premises
- Ensure images are securely stored and retained for 28 days
- Access to live images is only by authorised staff
- Apart from law enforcement bodies, images will not be given to third parties
- Respond appropriately to those wishing access to their own images
- Check the system annually

4.10 Retention, destruction and disposal

Records containing personal information should not be kept longer than necessary. See Appendix 5 for details.

Arrangements for storage/archive of records and information must be made at departmental level.

Records that need to be destroyed should be shredded on site, where this is not possible they need to be identified and stored in a secure location – for eventual destruction.

Destruction of confidential records must ensure that their confidentiality is fully maintained. Normally destruction should be by incineration or shredding.
The destruction of the records must be witnessed by a SNHC employee.

A permanent record must be kept of the records that have been destroyed

Measures should be taken to ensure that:

- all software and data is removed from redundant hardware and media storage (e.g. tapes, disks) before the hardware is removed from the Trust.
- confidential (any information containing personal data) paper waste is shredded or is collected and held in a secure area prior to shredding/incinerating.

Disposal of non-clinical waste
SNHC has a legal obligation to maintain confidentiality standards for all information relating to patients, employees and Trust business. It is important that this information is disposed of in a secure manner.

All employees will be made aware of how easy it is to breach confidentiality by incorrect use of waste paper, by using examples of ‘real life situations’ during training sessions.

4.11 Reporting of Data Management Policy Breaches

All events involving actual or suspected breaches of this Data Management Policy must be treated as incidents and handled in accordance with the Information Incident Reporting Guidelines, contained within Appendix **8** of this Policy. Breaches may include failures of information security safeguards, violations of confidentiality, loss of personal or sensitive information, or unexpected events which could or do lead to business disruption.

5. Related Policies / Guidelines

Consent Policy
Health and Safety Policy
Disciplinary Policy

6. Monitoring and Review

This policy will be reviewed every 2 years or more often if legislation or national guidance changes.

7. Statutory Compliance and Evidence

Access Modification (Health) Order
Access to Health Records Act
Caldicott Report
CCTV Code of Practice
Computer Misuse Act
Data Protection Act
Data Protection Good Practice Note - Charities and marketing
Freedom of Information Act
Health and Social Care Act (section 60)
Human Rights Act
Mental Capacity Act
Privacy and Electronic Communications
Public Interest Disclosure Act ("Whistle blowing")
Public Records Act

8. References

The Information Commissioner's Office

9. Appendices

Appendix 1 Guidance on maintaining confidentiality

Below are some basic rules on maintaining the confidentiality of personal information.

Manual records
They should be stored securely in locked rooms or cabinets. Confidential information such as patients' records must not be left lying around in accessible areas such as reception desks where they may be viewed by members of the public or unauthorised staff.

Electronic records
Access to any PC must be password protected, this must not be shared. Computer screens must not be left on view so members of the general public or staff who do not have a justified need to view the information can see personal data. PCs or laptops not in use should be switched off or have a secure screen saver device in use. Laptops/hand held devices to be kept secure in locked rooms or cabinets or in a safe environment (where members of staff are present at all times). The information must be password protected.

Telephone enquiries
When telephone enquiries are received asking for disclosure of personal information, the caller should be asked to put their requests in writing where applicable. Where requests have to be dealt with more quickly, the following rules must be adhered to:

- The disclosure is legally justified and the caller has a legal right to access that information
- You are certain the caller is who they say they are, you can confirm this by carrying the following checks:
- Verify personal details.
- If the caller is part of an organisation/company, you should obtain the main switchboard number of that organisation (via phone book or directory enquires) and ring back.
- Always provide the minimum amount of information that is necessary.
- If in doubt, tell the caller you will ring back. Where necessary consult a senior manager or the designated authority for confidentiality issues within SNH.
- All press enquiries for example should be directed to the Chief Executive's Office at SNH.

Answer phones
You must only leave a message on a patient or individuals answer phone if it is urgent. If this is the case, leave your name and number only – do not say it is SNH calling.

Transfer of Personal Data
The 7th principle of the Data Protection Act requires that appropriate technical and organisational measures shall be taken against accidental loss of personal data. Experience shows that the greatest risk of accidental loss arises while data is being transferred. Careful consideration should be given to the most appropriate method of transferring data taking into account the nature of the information and the degree of harm that could result from its accidental loss or disclosure.

This section of the Data Management Policy defines the circumstances in which each transfer method can be used, and provides details of the processes to be adopted. Where there is any doubt about the interpretation of these procedures, or confusion about the correct course of action in any specific circumstance, guidance should be sought from the Information Governance Lead.

External and Internal Post/Courier

Personal data can be sent via external post (typically Royal Mail), NHS transport or courier. The data can either be in paper or electronic form. There are a number of measures that should be taken whichever transfer medium or format is used:

- Ensure that packages/envelopes are addressed correctly; confirm the name, department and address of the recipient and ensure that these details are marked correctly on the item. Where possible window envelopes should be used, as these mitigate the risk of personal information being sent to the wrong recipient

- Mark the package/envelope 'Private and confidential' and include a return address where this will not compromise confidentiality

- Consider the weight of the items when selecting a packaging method – ordinary office envelopes are easily damaged in transit, allowing confidential items to be lost or disclosed. Tamper-evident plastic mailing bags provide assurance that the items have remained secure in transit as well as being inherently stronger than paper equivalents.

For items in paper form, consideration must be given to the type and volume of the data when deciding on the appropriate transfer method. For any communications with organisations who use the NHS transport service provided by Norfolk and Suffolk Foundation Trust this should be the default method; there is no transaction cost, and it can be considered secure.

For other organisations or individuals, it is not possible to provide definitive guidance for every circumstance. The following examples will illustrate the considerations that will have to be made.

- Routine communications with patients that do not contain substantial amounts of detailed personal information, the disclosure of which is unlikely to cause distress, can be sent by ordinary Royal Mail post.

- Bulk transfers of personal data, or detailed clinical information such as patient records should be sent by a method that permits tracking of the item in transit, as well as proof of delivery.

Where the item is in electronic form, such as a USB memory stick, a memory card, a portable hard disk drive or a CD/DVD ROM, there are additional specific measures that must be taken to protect the data, in addition to the general measures outlined above.

- The data on the device must be encrypted, to a standard that meets NHS Information Governance requirements.

- The password to decrypt the data must be sent to the recipient by completely independent means; it completely defeats the object of encrypting the data if the password is included with the media.

Email

Personal data should not be sent by email except under the following circumstances:

- When an NHS Mail account is being used to send to a recipient who also has an NHS Mail account – i.e. where the recipient's address is in the form 'name@nhs.net'. In this case, both the sending and receiving processes are automatically encrypted.

- Where the personal data is manually encrypted before sending. This capability is available on a restricted basis within the Hospice. Users with a business need to encrypt personal data should contact the Information Governance Lead for further details. The password to decrypt the personal data should be sent by completely independent means, not included within the email.

In practice, it is far more common for personal data to be inadvertently disclosed by the email being incorrectly addressed, than by being intercepted. For this reason, the recipient's email address should always be confirmed before sending personal data. This applies particularly to NHS Mail accounts, where no intervention is required to decrypt and read the email. No reliance should be placed on the force of the Hospice's email disclaimer.

Fax

The use of fax machines for sending personal data should only be considered where there is no more secure alternative. When this method is used, the following conditions must be adhered to.

- Where the communication is likely to be regular, the number should be pre-programmed into the fax machine's memory and accessed by speed-dial. The number should be tested before using it to send personal data
- A reasonable attempt should be made to confirm that the fax is being sent to a safe location, where only staff who have a legitimate right to view the data can access it
- Where communication is likely to be infrequent and it is not appropriate to use a previously stored number, additional precautions should be taken:
    - Care should be taken to confirm that the correct number is being used
    - The sender must contact the recipient before sending the fax
    - The sender must request confirmation that the fax has been received. If confirmation is not received, the sender should contact the recipient for confirmation.
- In either case, the receipt provided by the sending fax should be checked to confirm that the receiving fax number, as indicated by the Caller Line ID, is correct.
- The receipt should be retained for future checking

Overheard Conversations
Where conversations are conducted by staff relating to SNH business either over the phone, face to face or in the close proximity of public/receptions areas, care must be taken that personal information is not overheard by persons who do not have a right or need to hear such information. This can also apply where recorded messages are re-played. Where departments or practices feel there is a definite problem, procedures should be implemented to improve the situation.

Information sharing
Information must not be shared with other staff or with their family, carers or other persons without the express permission of the patients/client. The only exception to this shall be where it is necessary to share information to protect the health and wellbeing of

the patients/client or of others. Such disclosure must be limited and appropriate. A note of such disclosure, the date, purpose and recipients, together with any record of consequence or response must be added to the patient/client notes within 24 hours of the disclosure.

Should information be passed to an authorised person, internally or externally, those sharing it must ensure the identity of the recipient and that they have a valid need for the information, are aware that it is confidential, and will deal with it appropriately and safely.

It may be necessary for essential personal information to pass between the SNH, NHS, Local Authority, Social Services and other services. This may happen for example where one of these services is contributing towards a programme of care. Where information sharing takes place, a protocol arrangement should be in place which gives SNH necessary guarantees on the security of the data.

Appendix 2 Guidance on completing health records

Completion of Health Care Records Guidelines

1. Introduction

These guidelines are pertinent to all those who contribute to the professional care of patients and their families including administrative staff, students, volunteers and non-professional carers. It was developed by Jackie Saunders, Clinical Services Director in consultation with Jo Francis RN, Jane Creed RN, clinical colleagues following training events and consultation with Andrew Newman, volunteer legal advisor to the Hospice.

2. Why important?

The Courts of Law approach to record keeping tends to be that 'if it is not recorded, it has not been done'. Record keeping is central to health and social care practice. It is integral to the planning and delivery of care and is not an optional extra to be fitted in if circumstances allow.

A healthcare record is anything that contains information which has been collated as part of the work of an employee or volunteer pertinent to describing or noting interventions, opinions or plans regarding patients or clients. It usually refers to written material (handwritten or typed) but also includes audio, photographic and computer based records (free-text and numeric)

Good record keeping helps to protect the welfare of patients/clients by promoting:

- High standards of clinical care
- Continuity of care
- Communication and dissemination of information between members of the multi-professional team
- An accurate account of treatment and care planning, delivery and evaluation
- The identification of risks and detection of problems, such as changes in the patient /client's condition at an early stage.

Staff have both a professional and a legal duty of care; they are responsible for any records they create or use. Their record keeping must demonstrate:

- Evidence they have understood and honoured their duty of care, that all reasonable steps have been taken to care for the patient/client and that any actions or omissions have not compromised the patients safety in any way
- They practice within the law and their professional framework
- They observe the common law duty of confidentiality.

3. Patient, client and carer involvement

Patients and clients will be informed about the purpose of hospice records, and that other hospice multidisciplinary team staff *involved in their care* have access to the records. They must be informed of the uses to which information about them and any record of treatment may be put, together with any intended disclosure to outside agencies or persons as per Consent Policy.

Patients and clients must be equal partners, whenever possible, in the compilation of their records. What is written must, whenever possible, be constructed with the involvement of the patient/client or their carer. This is particularly pertinent to the issues of consent and “Thinking Ahead” recording. Their feedback/comments regarding the assessment, treatment and care plan must be noted.

4. Who contributes to Health Care Records?
Any member of clinical staff [*]can contribute to the Records and can write in any part of the notes as long as they are competent to have either assessed, planned, delivered or evaluated care. Important issues communicated with patients or carers must also be recorded.

Volunteers and students must have their entries counter-signed by a qualified professional. Care Assistants write about their actions taken and observations made; they do not need their entries countersigned.

5. Content and style
Staff are required to use their professional judgement to decide what is relevant and what must be recorded. There are a number of factors that contribute to effective record keeping. Records must be:

Factual, consistent and accurate.
Focused on the what, where, when, who, why and how.

Complete with clear evidence of the

- patient/clients aspirations of care,
- staff goals,
- care planned
- decisions made,
- care delivered
- information shared
- weighing of risks and benefits
- rationale for intervention
- interventions which have been deliberately avoided to prevent harm / because of futility
- identification of risks and/or problems that have arisen and the action taken to rectify them
- contacts and relevant events
- cross reference to other records held e.g. Family Support counselling and family notes. Information must be consistent between the records.
- judgments or decisions made
- staff involved in any joint decisions

Easy to follow

- with clear filing instructions for all sets of records.
- written chronologically within subsections, not just by discipline or department.
- documents filed in date order, in the correct section.
- sections must be used unless Records are short.
- free from abbreviations
- free from jargon, meaningless phrases, irrelevant speculation, offensive or subjective statements, or humorous comments about patients/clients or staff.

Recorded as soon as possible after an event has occurred providing current information on the patient/client.

Written in the first person when recording actions taken. It is appropriate to document personal opinion as long as it is written as such.

Timed and dated using a 24 hour clock (e.g. 1400hrs not 2pm). Some entries require both a start and an end time. Dates must be UK (day/month/year) not USA (month/day/year) style.

[*] "Staff" includes those with honorary contracts such as honorary Chaplains and sessional workers.

Signed with printed name and designation

- dictated notes must be checked, corrected and signed by the author. Dictated letters can be signed *per procurationem* by a fellow professional of the same discipline.
- clinical results/reports must be checked and signed before filing. Abnormal results must be highlighted in the record, and action taken documented.

Permanent using black ink which cannot be erased and can be photocopied or scanned.

- Errors must be scored out with a single line and the correct entry written alongside, with the date, time and signature.
- On 'lined paper', such as our MDT note sheets, blank lines must not be left. Where gaps or empty lines are left, this space must be crossed through with a black line.
- Justifiable alterations or additions are dated, timed and signed or clearly attributed to a named person in an identifiable role in such a way that the original entry can still be read clearly.
- Amendments to Controlled Drug recording must be indicated by (…) being put round superseded entry, dated and signed; this is different to the single black line used to score out text.

Secure all pages must

- be held securely in the record to prevent detachment.
- have the name of the patient/client, and identification number and/or other unique identifier

Constructed well The pre-printed proforma must discourage duplication of information

Readable basic forms must only be photocopied from master copies available on S:drive –

Complaint, compliment and litigation correspondence must not be filed in the records.

Alerts must not be placed on the outer cover of the Health Care Records to prevent breach of confidentiality.

Appendix 3 Guidance on accessing health records

Procedure to access health records

1. Applications for access should be made in writing or electronically to the Chief Executive

2. If there is an application for access to a patient's clinical notes, the Clinical Services Director must be informed as soon as possible. It is the responsibility of the Clinical Services Director to co-ordinate the response to all such requests, liaising with the Chief Executive as Data Controller.

3. On receiving a request in writing from a person or their representative, the Clinical Services Director should immediately examine it to confirm its validity as part of best practice, and open a file to record all communication regarding the application.

4. Withholding information

   Under the Data Protection Act 1998 there are certain circumstances in which the record holder may withhold information. Access may be denied, or limited, where the Clinical Services Director judges that information in the records would cause serious harm to the physical or mental health or condition of the patient, or any other person, or where giving access would disclose information relating to or provided by a third person who had not consented to the disclosure. The Clinical Services Director will be able to justify decisions to withhold information, but is not obliged inform the applicant of the reason.

5. Once the Clinical Services Director has all the information she needs to deal with the request she should then consult the appropriate health professional, normally the individual who is or was responsible for the clinical care of the patient during the period to which the application refers.

Individuals who lack capacity – Mental Capacity Act 2005

1. In line with the Mental Capacity Act 2005 every effort should be made to assist a person in decision making and this includes understanding and giving consent for the disclosure and sharing of information about them. Consideration should be given to whether the decision needs to be made immediately or whether the person will be able to understand the nature of an information request at a later date

2. **Lasting Power of Attorney** – (LPA) The Mental Capacity Act 2005 creates a new Lasting Power of Attorney that enables individuals to appoint others to act on their behalf in decision making situations when they are not able to do so. The LPA for welfare matters comes into force when the individual is deemed to lack capacity for whatever welfare or care decision is being made. The LPA also grants the holder a right of access to information.

3. Once it is deemed the patient lacks capacity and it is deemed in the best interests of the patient to share information the holder of the LPA will be required to provide a copy of the LPA papers to ensure the Trust is satisfied it will meet its statutory requirements. The LPA must be registered with and stamped by the Court of Protection. More information can be sought from The Office of the Public Guardian http://www.publicguardian.gov.uk/ It should be noted that this is not an express right to have access to the full record of another, only what is considered relevant material and deemed to serve the best interests of the patient should be disclosed.

4. For those individuals who may lack capacity and family members or carers do not hold an LPA, decisions about information sharing should always be considered under best interest principles and with the ongoing relationship between the Trust the patient, and family or carers in mind

Applications made by someone other than the patient

1. Where the applicant is not the patient, the applicant should have access to only the information and explanation which would otherwise have been made available to the patient.

2. A request from a solicitor acting on behalf of a patient should be dealt with in exactly the same way as a request from a patient.

3. The Clinical Services Director, in conjunction members of the clinical team and the Chief Executive then should decide if the applicant should access their records under supervision of an administrator or health professional. Any abbreviations or intelligible notes should be explained.

4. If requested by applicant or representative original versions of the records should not be sent. The Data Protection Act allows an applicant to see a copy of, not the original health records.

5. The time limit for access is as follows:
   a. Once the Clinical Services Director has all the relevant information, they should comply with the request promptly and within 21 days, though in exceptional circumstances this may take up to 40 days. The 21 day limit is Department of Health policy, not a legal obligation.
   b. The request should be met within the 40 day limit is requirement under the Data Protection Act 1998. In exceptional circumstances if it is not possible to comply within this period the applicant should be informed.

6. Making amendments
   a. If a patient feels information recorded on their health record is incorrect then they should firstly make an informal approach to the health professional concerned to discuss the situation in an attempt to have the records amended. If this avenue is unsuccessful then they may pursue a complaint under the Hospice Complaints procedure in an attempt to have the information corrected or erased.

   b. They could further complain to the Information Commissioner, formerly the Data Protection Commissioner, who may rule that any erroneous information is rectified, blocked, erased or destroyed. Further information can be obtained from the Commissioner at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, telephone number 01625 545700.

7. Charges for access to health records
   a. Under the Data Protection Act 1998 (Fees and Miscellaneous Provisions) Regulations 2001

8. Maximum fee that can be charged for providing copies of health records is £10 for computer records

9. £50 for copies of manual records or a mixture of manual and computer records.

a. Charges are for copying and posting the records only and should not result in a profit for the record holder. Some types of records, such as x-rays, may be expensive to copy.

b. The Clinical Services Director can waive if the charge at her discretion.

Access to Deceased Patients' Records

1. Health records relating to deceased people do not carry a common law duty of confidentiality. However, it is Department of Health and General Medical Council policy that records relating to deceased people should be treated with the same level of confidentiality as those relating to living people. Access to the health records of a deceased person is governed by the Access to Health Records Act 1990.

2. Under this legislation when a patient has died, requests for access to the deceased's health records can only be made by:
    a. A patient's personal representative (the executor or administrator of the deceased person's estate)
    b. Anyone having a claim resulting from the death (this could be a relative or another person)

3. For any request for deceased patient records health professionals should take into account the following points before release:
    a. The wishes of the patient while they were alive
    b. Any potential harm to relatives or other persons by releasing information

Appendix 4 Guidelines on use of Information Technology

Prohibited Use

The following list is not exhaustive, but is provided as an indication of prohibited use:

- Deliberately viewing or sending any pornographic, obscene, indecent or non-clinical sexually explicit, illegal or offensive/discriminatory material.
- For any commercial activities (e.g. running a business)
- To perpetrate any form of fraud or criminal activity.
- For personal financial gain
- Bring the organisation or a colleague into disrepute.
- Any form of defamation, discrimination, harassment or bullying.
- Where it interferes with the work of the individual, colleague, department or business of the organisation.
- For illicitly distributing any patient or business confidential material.
- For hacking or gaining access to unauthorised areas.
- For the deliberate introduction of viruses, spyware or malware.
- The use of proxy avoidance websites.
- Streaming video or audio for non-work use.

In order to monitor compliance with these guidelines, the use of the Internet and email may be monitored without further notice.

Passwords

When allocated a new/temporary password for start-up use by the systems manager/ administrator the user must immediately change it

Passwords

- Should be formulated in such a way that they are easily remembered but difficult to guess and should be formulated using letters (upper and lower case), figures and other characters.
- Must not be displayed on screens as they are entered
- Must consist of a minimum of 8 characters and for strong passwords should also include 2 numbers and capitals as part of the 8 characters
- Must be changed on change of staff or staff resignation
- Must not be shared amongst users
- Must not be written down
- Should not relate to the system or the user, although passwords must be easy to remember
- Must be changed regularly, at intervals not exceeding 90 days

Email Guidance

1. Use e-mail only for work related purposes. A small amount of personal email will be permitted providing this is not misused.
2. Note that e-mails may be monitored without notice.
3. Obtain confirmation of receipt for all important e-mails sent.
4. Make and keep hard copies of all important e-mails sent and received.
5. Check your e-mail on each working day or arrange for a duly authorised person to do so on your behalf by granting the appropriate permissions – NOT by sharing your password.
6. For any period of absence set an out of office message and during any long period of absence set a redirection for your emails for the period of your absence.
7. Exercise caution when drafting e-mails. Be aware of the potential contractual implications; e-mail can be considered a legally binding contract.
8. Use the most up to date (available from the marketing department) email footer and disclaimer for external mail

Do Not:

- Use e-mail as a substitute for speaking to people.
- Send messages from other people's computers in their name without authority to do so.
- Circulate chain letters or mass mailings.
- Copy e-mails to large numbers of people for information unless absolutely essential.
- Use the e-mail footer for internal mail
- Include confidential data within an email – e.g. personal data, credit card information etc unless it is encrypted. This restriction applies to internal as well as external emails

Use of attachments

- Exercise vigilance when accessing attachments, especially from unknown sources. E-mail is the most common method of transfer of computer viruses and malicious programmes.
- Limit the use of large attachments – wherever possible provide a hyperlink to folders or websites
- Be aware of the copyright rules

Housekeeping

- Keep the number of emails that are not dealt with to a minimum
- Empty inbox daily and file emails into folders
- Archive and delete deleted and sent emails regularly

Do Not

- Retain emails with large attachments

Appendix 5 Retention Schedule

Retention schedule.xlsx

Appendix 6 Photographic Consent Forms - Adults

PHOTOGRAPHIC CONSENT FORM – Adults

St Nicholas Hospice Care would like to use a photographic/video image(s) of you for the purposes of promotion and marketing of the Hospice and in fundraising materials. We would like to publish this image(s) in any form of media now known (including website) or developed in future. Please note that your name will not be published with the image(s) without your prior consent. Before taking or using any photographs or video of you we need your permission. Please complete this form and then sign and date where indicated.

Your personal details

Surname.....

Forename(s).....

Address.....

.....

.....

Telephone number.....

Thank you for allowing us to use this image. Are you happy for us to use this image:

For one occasion only ☐

For 5 years from today ☐

In perpetuity ☐

Do you permit us to publish your name with the image(s)?

Yes ☐ No ☐

Declaration

I agree to St Nicholas Hospice Care using my photographic image in all media now known and hereinafter devised throughout the World for a period as stated above.

Signature..... Date.....

Please note that St Nicholas Hospice Care will process the personal information provided in this form in accordance with the Data Protection Act 1998 and will use it in the management of its photographic resources.

For office use:
Image number: Link to image:

Use of image, if one occasion only .....

Appendix 7 Photographic Consent Forms – Children

serving the local community

St Nicholas Hospice Care

A Registered Charity No. 287773

PHOTOGRAPHIC CONSENT FORM – Children

St Nicholas Hospice Care would like to use a photographic/video image(s) of your child for the purposes of promotion and marketing of the Hospice and in fundraising materials. We would like to publish this image(s) in any form of media now known (including website) or developed in future. Please note that your child's name will not be published with the image(s) without your prior consent. Before taking or using any photographs or video of you we need your permission. Please complete this form and then sign and date where indicated.

There have been concerns surrounding the risk of a child or young person being identified as a result of an image(s) appearing in the media. St Nicholas Hospice Care takes the view that the risk of a child being identified by a stranger is small and that, providing reasonable steps are in place in terms of the appropriateness of the image(s) and to protect the full name and contact details of children or young person, photography will be permitted. If there are any specific reasons why a child's identification is a matter of particular anxiety, either now or in the future, that would affect or change your consent on this issue please contact us.

Childs/Young Person's personal details
To be completed by the parent or guardian

Surname.....

Forename(s).....

Address.....

.....

.....

Telephone number.....

Thank you for allowing us to use this image. Are you happy for us to use this image:

For one occasion only ☐

For 5 years from today ☐

In perpetuity ☐

Do you permit us to publish the child's/young person's name with the image(s)?

Yes ☐ No ☐

Declaration

I agree to St Nicholas Hospice Care using the child's/young person's photographic image in any form of media now known (including website) or developed in future, for a period as stated above.

Signature of Parent or Guardian.....

Name of Parent or Guardian (in block capitals).....

Date.....

Please note that St Nicholas Hospice Care will process the personal information provided in this form in accordance with the Data Protection Act 1998 and will use it in the management of its photographic resources.

For office use:
Image number: Link to image:

Use of image, if one occasion only .....

Appendix 8 Guidelines on identifying and reporting information incidents

These guidelines apply to all staff including permanent, temporary, and bank members of staff, and to volunteers. All incidents must be reported to your line manager and/or St Nicholas Hospice Care's Information Governance lead as soon as possible after the event.

What should you report?
Here are some examples of information incidents that should be reported:

- Finding person-identifiable information from the organisation in a public place
- Identifying that a fax containing person-identifiable information has been sent to the wrong destination;
- The loss of an unencrypted laptop computer with personal information on it;
- The transmission of information to someone who should not have access to it – orally, in writing or electronically;
- Access to information using someone else's authorisation e.g. someone else's user id and password;
- Access to person-identifiable information by a member of staff or volunteer using another person's credentials or smartcard;
- Identifying that a PC and/or programme isn't working correctly – potentially because of a virus;
- Sending a sensitive e-mail to 'all staff' by mistake;
- Finding a colleague's password written down on a 'post-it' note;
- Discovering a 'break in' to an organisation building or car.
- Finding confidential waste in a 'normal' waste bin.

How should you report an incident?
If you discover something that could be considered as an incident you should report it to your manager and complete the Information Incident Report form. Full details of the Incident Reporting Procedure can be found in Appendix 2 of the Health and Safety Policy.

What happens next?
The manager responsible for the area or service in which the incident occurred will investigate the incident and may wish to speak to you directly as things progress.