Information Governance & GDPR Policy

Authors:	Joy Farquharson/Bruce High
Chief Executive	Joy Farquharson
Deputy Chief Executive: Patient Services	Margaret Wilkie
Quality & Governance Manager	Wendy Cowper
Implementation Date:	Oct 2022
Version Number:	3.1
Review date:	October 2024
Responsible Committee:	Information Governance

Contents

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Bruce High • Joy Farquharson • Wendy Cowper • Margaret Wilkie
Consultation Process / Stakeholders:	• Information Governance Committee • Integrated Governance Committee
Distribution:	• All Hospice departments via SMI. A copy of all policies will be held centrally on the shared drives.

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
August 2015	Bruce High	Draft - First Catalogued Version of this policy.	0.1
May 2018	Joy Farquharson	Amended to reflect change from Data Protection Act to GDPR	2.0
Oct 2022	M Wilkie/W Cowper	Mandated Review	3.0
Feb 2023	J Farquharson	Text changes Head of People/Facilities Mgr. Process review	3.1

1. Introduction

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources including staff and volunteers. It plays a key part in service planning and performance management. Information is also of vital importance for fundraising purposes on which the Hospice is reliant.

It is therefore of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures and structures provide a robust governance framework for information management.

Personal data at St. Andrew's Hospice can include employees and volunteers (present, past and prospective), patients, contractors and third parties, private and confidential information as well as sensitive information, whether in paper, electronic or other form.

Irrespective of how information is collected, recorded and processed person-identifiable information must be dealt with properly to ensure compliance with General Data Protection Regulations (GDPR).

2. Aim and Purpose

St. Andrew's Hospice (SAH) has a duty of care to patients, staff, volunteers and donors as well as a duty to support professional ethical standards of confidentiality. This policy aims to ensure information is managed appropriately with regard to the privacy of individuals, in line with the requirements of the General Data Protection Regulations 2018 and Caldicott Principles.

The objectives of SAH Information Governance Policy are:

- Information will be protected against unauthorised access.
- Confidentiality of information required through regulatory and legislative requirements will be assured.
- Integrity of information will be maintained.
- Information will be available to authorised personnel as and when required.
- Regulatory and legislative requirements will be met.
- Business Continuity Plans will be produced, maintained and tested.
- Confidentiality, Data Protection and Security guidance will be in place.
- Information security training will be available to all staff.
- All breaches of information security, actual or suspected, will be reported to line management and an investigation will be undertaken if necessary.
- Identification of a Data Protection Officer

3. Scope

3.1 Who is the Policy intended to Benefit or Affect

This policy will benefit both patients, their families, staff, volunteers and donors as information is held by the organisation of all of these groups. All require to be held under the terms of the General Data Protection Regulations.

3.2 Who are the Stakeholders

The stakeholders are anyone within the organisation who has responsibility for collecting and storing information about patients, their families, staff, volunteers or donors.

3.3 What is covered by this policy?

This policy is an overarching policy and together with the policies/procedures in the table below covers all aspects of handling, transferring, storage and destruction of information, including paper and electronic structured record systems, the transmission of information using fax, e-mail, post and telephone, some of which are governed byt NHS Lanarkshire policy as highlighted below.

Record of Information Governance Policies	Author
Disclosure Handling Policy	SAH
Professional Boundaries Policy	SAH
Social Media Policy	SAH
Access to Health Records Policy	SAH
NHSL Information Security	NHSL
NHSL Information Security Computer Asses Mgmt and Tracking	NHSL
NHSL Information Security Policy Email Usage	NHSL
NHSL Information Security Policy Acceptable use of Removable Storage Devices	NHSL
NHSL Information Security Policy Data Protection	NHSL
NHSL Information Security Home Working Policy	NHSL
NHSL Information Security Fraud Policy	NHSL
NHSL Information Security Intranet Usage Policy	NHSL
NHSL Information Security Remote Access Policy	NHSL
NHSL Information Security Internet Usage Policy	NHSL
NHSL Information Security Wireless Connectivity Policy	NHSL
NHSL Information Security Secure use of Systems Policy	NHSL
NHSL Information Security Secure use of Passwords Policy	NHSL
NHSL Information Security Secure use of Data Network and Internet Services	NHSL
NHSL Information Security Secure use of Personal Computers	NHSL

4. Principle Content

4.0 Definitions:

The GDPR defines personal data as the following:

"Personal data means any information relation to an identified or identifiable natural person ('data subject') is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location number, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Data which was called 'sensitive personal data' under the Data Protection Act is now referred to as Special categories of personal data and are classified as:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Generic data and biometric data
- Health
- Sex life and sexual orientation

Data Controller – "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". For SAH this is the Board of Trustees

Data Processor – "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". For SAH this means an external organisation who processes data on our behalf.e.g. Lottery Canvasing Company, Mailing Companies etc.

4.1 IT Asset

IT hardware and software will be provided to staff and volunteers who require this equipment to facilitate and support their role. SAH IT equipment is provided for business purposes only and not for personal purposes for example email, internet access, social network, gaming etc. SAH reserves the right to monitor IT usage, including internet access, and any breach of confidentiality or inappropriate use will be investigated and may result in disciplinary action being taken against the staff member.

4.2 Information Security

The objective of Information Security is to safeguard the confidentiality, integrity and availability of all forms of information within SAH. Information is one of our most valuable assets and it is essential that we have adequate safeguards to ensure that it is not lost or compromised. The SAH data may be extremely personal to patients, staff, volunteers or donors. Patient data may influence the treatment patients receive and may be required reliably and urgently.

4.3 Principles

4.3.1 The Principle of Openness

Like the Data Protection Act the GDPR covers the processing of personal data- this includes all automated and manual processing of personal data that will be kept as part of a structured system.
The law does not apply to:

- the processing of personal data by individual for purely domestic or household reasons,
- To the processing of data for purposes of national security
- The processing of person data by certain authorises for the purposing of preventing, investigating detecting or prosecuting criminal offences

As with the current law, GDPR only applies to the processing of personal data of living data subjects.

The Hospice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Information is defined and where appropriate kept secure, underpinning the principles of Caldicott and the regulations outlined in the General Data Protection Regulations2018.

Non-confidential information on Hospice services is available to the public through a variety of means and patients have access to information relating to their own health care treatment options and their rights as patients.

With the patient's stated and documented permission, carers and family members can be provided with information in terms of diagnosis, prognosis, treatment and care. This information will be given as appropriate and with respect for patient confidentiality. Where a patient lacks capacity (Adults with Incapacity Act) consent will be sought from their Power of Attorney or in the case of guardianship, the appointed person.

The integrity of information is monitored and maintained to ensure that it is fit for the purposes intended. The Hospice will ensure that it treats personal information lawfully and correctly. To this end the organisation fully endorses and adheres to the Principles of Data Protection as set out in the General Data Protection Regulations.

4.3.2 The Principles of General Data Protection Regulations.

The Act stipulates that anyone processing personal data must comply with eight principles of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. Lawfulness, fairness and transparency

…processed lawfully, fairly and in a transparent manner in relation to individuals;

2. Purpose Limitation

…collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. Data Minimisation

…adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Accuracy

…accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

5. Storage Limitation

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

6. Integrity & Confidentiality

…processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

In addition in Article 5(2) GDPR introduces an entirely new accountability principle:

7. Accountability

…the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Subject Access Rights

The GDPR builds on the current law by enhancing existing data subject rights and adding a number of entirely new data subject rights. In addition, organisation cannot longer charge a £10 fee for subject access requests and must response with 28 days. (Please see Subject Access Request Standard form, appendix 1)

Individuals have the right to obtain the following from SAH:

- confirmation that we are processing their personal data;
- a copy of their personal data;

In addition to a copy of their personal data, SAH also have to provide individuals with the following information:

- the purposes of our processing;
- the categories of personal data concerned;
- the recipients or categories of recipient we disclose the personal data to;
- Our retention period for storing the personal data or, where this is not possible, your criteria for determining how long we will store it;

- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards we provide if you transfer personal data to a third country or international organisation.

Some of the above information is provided in our privacy notice. (See Appendix 1)

Data Protection Officer

To allow SAH to carry out its Core Business (providing specialist Palliative Care) we required to collect, process and store Special categories of Personal data on a large scale meaning we are therefore requiring to appoint a Data Protection Officer.

This role will be a responsibility of the Quality & Governance Manager and the following has been put in place to allow them to fulfil their role:

- Received training of data protection law and practice
- Is involved properly and promptly in all issues which relate to data protection of personal data
- Reports directly to the Deputy Chief Executive
- Will independency report to the board of Trustees bi –annually
- Will not be dismissed or penalised for performing their role as Data Protection Officer

The Data Protection Officer is specifically responsible in line with Article 39 of the GDPR for:

- To inform and advise on compliance with GDPR and other data protection laws
- To monitor compliance with the law and any internal polices, including assigning responsibilities, awareness raising and training staff
- To advice on and monitor data protection impact assessment
- To cooperate with and act as a point of contact with the supervisory authority (ICO)

4.3.2` The Principles of Caldicott

The appointed Caldicott Guardian is responsible for ensuring that staff members recognise their professional and legal responsibility in maintaining patient confidentiality in accordance with the following Caldicott Principles:

- Justify the purpose for transferring confidential information
- Don’t use patient information unless it is absolutely necessary
- Use the minimum necessary patient identifiable information
- Access to patient information is on a strict need to know basis
- All staff members / volunteers are aware of their responsibilities in respect to patient information
- Understand and comply with the law
- Information is kept secure at all times
- Information is not kept longer than is necessary.

The Caldicott Guidance is currently the Deputy CEO/Head of Clinical Services. The Caldicott Guardian will undertake formal training at least every three years

4.4. Secure Transportation of Person Identifiable Data (PID)

It is imperative that staff treat the transportation of personal and patient information in a confidential and secure manner. For all Patient, Staff, volunteers or donor personal information the following procedure should be followed:

- Patient or staff information should be placed in a sealed plain envelope, marked “In Confidence” to a named person.
- Transit envelopes should not be used under any circumstances for documents containing personal or sensitive information.
- Electronic transfer of information should only be through approved routes. Email correspondence involving PID should only be via NHS domains (this includes standrews.scot.nhs.uk domain). IT advice should be sought should there be any doubt about information security.
- If email is required outwith approved domains, the file should be encrypted and consent should be sought from the person being discussed.

4.5. Human Resources

4.6.1 Human Resources security for Employees, External Contractors and Volunteers

To ensure that the security needs of the St. Andrew’s Hospice are adequately covered, job descriptions must contain clear descriptors of information security roles and responsibilities; this requires descriptions on segregation of duties and the appropriate selection and training of personnel in relation to information security.

Externally contracted staff and volunteers shall be subject to the same policies relating to security as staff of the St. Andrew’s Hospice. Where their work relates directly to sensitive security issues, for example, computer maintenance staff, extra conditions should be imposed according to the risk exposure such as reducing access to sensitive information within IT systems as much is as practicable.

Prospective staff, contractors and volunteers shall be given a clear understanding of their responsibilities for information security so that the extent of their authorities are defined and understood.

Any failure to properly inform a staff member of his or her responsibility for security may leave the St. Andrew’s Hospice vulnerable when trying to subsequently enforce disciplinary action.

4.6.2 Human Resources security: screening

St. Andrew’s Hospice requires all new and existing staff (including volunteers) to satisfy the appropriate pre-employment checks prior to an offer to join the Hospice being made, and the individual commencing their new role, in accordance with Recruitment and Selection Policies and Procedures.

Staff and volunteers shall sign a Confidentiality Agreement as part of their initial terms and conditions. Data Protection training should be undertaken within one week of commencement. (Mandatory LearnPro Module)

Personnel files for staff and volunteers that contain evidence of any recruitment checks must be held securely. Any physical or documentary files will be held under lock and key. In all cases, access to such files – logical or physical – is restricted to HR Personnel and line managers only. The Head of People is the owner of this information, and is responsible for its security.

4.6.3 Human Resources security: terms and conditions of employment

The terms and conditions of employment shall state the responsibility of each staff member where there is an information security component. The terms may be amended if the role or scope of duties is changed during the employment period.

New staff shall be given a clear understanding of their role and responsibilities for information security by their line manager so that authorities are defined and understood.

4.6.4 Termination or change of employment

When a staff member terminates employment with the St. Andrew's Hospice or where a volunteer ceases to volunteer on behalf of the Hospice, all property belonging to St Andrew's Hospice must be returned.

In addition, the following must be actioned prior to final departure of a staff member:

- all work-related work privileges must be revoked;
- All systems access and communication accounts must be terminated.

This process is essential to ensure that access to sensitive information in a previous post is not accessible in a new post where this is not necessary.

4.6.5 Termination responsibilities

Prior to a staff member leaving, or to a change of duties, line managers must ensure that:

- the staff member is informed in writing that he/she continues to be bound by their signed confidentiality agreement;
- passwords are removed or changed to deny access;
- relevant departments are informed of the termination or change, and, where appropriate, the name is removed from authority and access lists;
- passwords allocated to the individual should be removed and consideration given to changing higher level passwords, to which they have access;
- reception volunteers and others responsible for controlling access to appropriate premises, are informed of the termination, and are instructed not to admit in future without a visitor's pass;

- where appropriate, staff working out notice are assigned to non-sensitive tasks, or are appropriately monitored;
- departmental property is returned.

4.7. NHSL Network

Arrangements for the staff of St. Andrew's Hospice to access NHS Lanarkshire's information systems and facilities should be based on a formal request to ensure that St. Andrew's Hospice can satisfy NHSL's security requirements.

If access to NHSL services are required, the request form can be accessed through the IT Manager. This form requires to be authorised by the appropriate line manager. The form will then be sent to NHSL and if appropriate, authorisation will be granted with the necessary accesses. Whenever staff are granted IT access for the first time they are required to read and sign that they agree to comply with NHSL's security policies identified in the table in 2 above.

4.8 Exchanges of information

When sensitive and/or confidential information is transmitted or despatched between different departments within the St. Andrew's Hospice, and between St. Andrew's and other bodies for example, Local Authorities it should be subject to formal protocols.

The protocols should include the following:

- management responsibilities for controlling and notifying transmission, despatch and receipt.
- use of appropriate labelling for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected.
- information and software ownership and responsibilities for data protection, software copyright compliance and similar considerations.
- any special controls that may be required to protect sensitive items such as encryption.

Similar standards must be applied to the exchange of information in "hard copy", so that the manual exchange of confidential information is subject to similar standards.

Agreed transport couriers must be used at all times. Packaging should be sufficient to protect the contents from any physical damage during transit, and should be in accordance with manufacturers' specifications.

Special controls should be adopted, where necessary, to protect sensitive information from unauthorised disclosure or modification.

When using software packages as Microsoft Word and Excel is it important that the information is not unintentionally divulged. Embedded patient identifiable and sensitive information in documents within graphs, pivot tables etc. must be treated with caution. Staff must ensure that when using data within checks must be made to ensure that such data is either anonymised or removed as appropriate. Staff must be trained appropriately in the

use of such systems to ensure that they understand the use of linked tables, embedded tables and how information must be secured.

4.9 Access Control

St. Andrew's Hospice is required to use access controls and other security measures to protect the confidentiality, integrity, and availability of any information processed by computers and communications systems, and to assure that individuals can be held accountable for information that is processed.

Each system must have an access control which details the following:

- who has access;
- what information they have access to;
- relevant legislation and any contractual obligations regarding protection of access to data or services;
- standard user access profiles for common categories of job.

System administrators must ensure that:

- users understand the level of access they have been given;
- access rights of users who have changed jobs or left must be immediately removed;
- they periodically check for, and remove redundant user IDs and accounts;
- redundant user IDs are not issued to other users.

4.10. Unattended equipment

When you leave a screen unattended, you should place the system in a secure condition. Most operating systems provide two methods of protection, one to allow you to lock the screen (CTRL+ALT+DEL in Windows) and the other to provide, through a timeout, a screen saver. Each has its place in protecting the system from misuse. Be aware of the following measures:

- terminate active system sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
- log-off PCs when the session is finished (i.e. do not just switch off the PC or terminal);
- secure PCs or terminals from unauthorised use by a key lock or an equivalent control, e.g. password access, when not in use;

4.11. The Electronic Patient Record

Appropriate staff will be able to log into the St. Andrew's Hospice Patient Management System (CrossCare) and will have access to the Electronic details of all current and previous patients. Staff will have a level of access based on their job role.

Staff must ensure that they only access the details of those patients essential to performing their job within the hospice. Staff will keep any information obtained from accessing a patient's record confidential.

Any staff found to be accessing a patient's details without due reason may be subject to disciplinary procedures.

The Quality & Governance Dept. are responsible for undertaking regular Information Security Audits of both Clinical and non-clinical areas

4.12 Clear desk and screen policy

Where appropriate, paper and computer media should be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.

Adequate secure storage must be made available to support the clear desk policy.

Incoming and outgoing mail points and unattended fax machines should be protected. Desktop printers, which have robust storage which allows them to continue to print a document even after a power cycle (e.g. switched off overnight), should also be protected.

All clinical systems should be logged out of and closed when not in use. No confidential information should be visible on an unattended screen and PCs should be left in a secure state when not in use.

4.13 Verbal Communication of Personal Identifiable Information

Care should be taken when discussing personal information about patients or staff to ensure that conversations are not inappropriately overhead. Disclosure of personal identifiable information in this way would constitute a breach of confidentiality.

When communicating personal information via telephone staff should satisfy themselves that the information is being shared appropriately and verify the identity of the caller. Best practice involves calling the recipient back on a verified number. Care should also be taken as to who may overhear telephone conversations.

Where possible, when discussing personal information, the names of patients / staff members should be omitted from the conversation; identity should be confirmed using the CHI number or similar.

4.14. Secure Storage of Personal Identifiable Information

Keep personal identifiable information physically secure at all times
Do not leave personal identifiable information unattended.

St. Andrew's Hospice operates a clear desk policy. All personal identifiable information should be locked away when not in use.

Rooms, cupboards, drawers containing personal identifiable information should be locked. Keys should be kept in a secure location.

Access to the personal identifiable information should be restricted to only those with a genuine "need to know".

Always consider anonymisation of information where possible. Information is said to be anonymised when identifiers; such as name, address, full postcode and any other detail that might identify an individual are removed[1].

If anonymisation is not appropriate consider coding the personal identifiable information, keep the code separately in a secure location.

Always use the minimum volume of identifiable information for your requirements.

4.15. Privacy Markings

Privacy markings should always be used on envelopes/packages containing personal identifiable information as follows:

'**Confidential - Clinical Information'** – for all patient identifiable information of a clinical nature.

'**Confidential - Personal Information'** – for personal identifiable information which should be opened by the addressee only.

4.16. Health Records

A number of handling and transportation packaging methods are employed for the secure transfer of physical health records within the St. Andrew's Hospice. These include:

a) Single record envopak carriers with seals,

b) Multiple record envopak carriers with seals,

c) Double brown paper envelopes,

d) Brown paper and string,

Transportation packaging methods employed must be fit for the purpose and take into account the type of information being transported in line with the policy guidance.

All health records that are not transferred using the internal mail system and are to be transferred out with the St. Andrew's Hospice using any of the transportation methods described above must be sent by Royal Mail 'Special Delivery' or an approved 'Special Courier' where information is recordable and traceable.

4.17. Personnel Records

The following procedure should be used when transporting staff personnel records:
Place record in sealed plain envelope or plain packaging

Ensure appropriate privacy marking is clearly visible on package (in this case **'Confidential – Personal Information'** and that the package is addressed to a named person.

[1] NHS code of Practice on Protecting Patient Confidentiality

Place this inside another plain package ensuring all that is shown on the front is the name and address of the recipient. In order not to attract attention to the package do not put a privacy marking on this outside wrapper.

4.18. Letters

Use of Window Envelopes

It is imperative to respect the privacy of the individual concerned and all staff must be aware of the necessity to ensure that no information, apart from the name, address and privacy marking, is visible through the window of the envelope.

4.19. Methods of Transport

Internal Mail

It is imperative that any records or files containing personal identifiable information are transported internally using one of the approved transportation and packaging methods above.

The Internal Mail System should be utilised whenever possible.

On no occasion should transit envelopes be used for the transportation of personal identifiable information.

Transported items that contain personal identifiable information must never be deposited and left unattended in areas that are not secure i.e. entrances, corridors, stairways.

Taxi or Courier

It may be necessary for patient identifiable records to be delivered by taxi or special courier. In such cases staff must ensure that they are using an 'approved' taxi or special courier company with which the organisation holds a contract for service.

Royal Mail

The recommended service used to transport personal identifiable information out with St. Andrew's Hospice is 'Special Delivery'. This service offers a tracking facility which allows the sender to check the safe arrival of the records.

Vehicles

During working hours – any records, files, notes or other correspondence containing personal information must be stored in a locked car boot.

If visiting a patient or staff member only the relevant paperwork should be removed – all other paperwork must remain locked in the boot.

Out with working hours - the best practice is to return all records, files, notes or other correspondence at the end of the day. However, it is recognised that this is not always practical. If paperwork has to be out overnight it should either be left in the locked car boot out of view or taken into the staff member's home. Staff will be supported in whichever decision they take providing the staff member does not compromise information security.

Where Hospice vehicles are used for the transportation of personal identifiable information items and the vehicle is parked on Hospice premises overnight, at the end of each day the vehicle must be emptied of all such items to a secure storage location.

4.20. Secure Disposal of Personal Identifiable Information

Documentation containing any personal identifiable information must be shredded or segregated and placed in 'Confidential Waste for Shredding' bags or. These bags are available from and uplifted by Facilities Services as and when necessary and it is their responsibility to carry out the controlled shredding process.

4.21. Information security incident management

A security breach must be reported using the Datix Incident Reporting System. All Information Governance Incidents will be reported to the information Governance Committee and the Integrated Governance Committee.

4.21.1 Reporting information security breaches and weaknesses

All incidents or information indicating a suspected or actual security breach or potential breach should be reported to the appropriate line manager.

The Quality and Governance Manager will investigate the incident or weakness, and assess the level of impact it presents to the St. Andrew's Hospice. If the suspected breach concerns an IT system, then the Business Owner of that system will be involved in the investigation.

It is essential that all breaches or potential breaches are reported and investigated in order that there are continued improvements in information security and the management of systems.

Incidents will be reviewed the Quality and Governance Manager and discussed with the Caldicott Guardian. The incidents will be reported at the Information Governance Committee meeting and will be include for discussion at the Integrated Governance Committee.

4.22. Business Continuity Management

St. Andrew's Hospice has a Business Continuity Plans in place which include the various IT systems within the Hospice. The provision of IT services cannot be guaranteed and therefore plans are in place to ensure the continuation of departmental services in the event of systems failure and downtime. It must not be assumed that loss of IT services is likely to be of only limited duration, e.g. in the event of fire, terrorist activity, explosion or water damage.

When completing Risk Assessment for each of the IT systems, Managers should assess how soon after the loss or destruction of a system the effects would become serious, and what the service impact would be. The assessment should be reviewed regularly in case the importance of the system has changed. The effect of any loss or destruction may vary according to the time of the week, month or year when it occurs. To ensure adequate business continuity at all times, the worst timing of any such loss or destruction should be considered.

The Business Continuity plan includes the following:

- a formal, documented, risk assessment of the criticality of each system, including the impact of the short, medium and long term loss of the system on business activities;
- identification and agreement of all responsibilities and emergency arrangements;
- documentation of agreed procedures and processes, what action needs to be taken while the relevant contracted supplier implements disaster recovery procedures;
- a formal assessment of how resilience and continuity will be achieved.

Resilience measures may include duplicating parts of the installation to reduce the risk of breakdown stopping its operation. Continuity measures may include falling back to a manual system or identifying alternative installations or sites to which the system can be moved if the computer is lost.

Multiple copies of each continuity plan, held both on-site and offsite. On-call staff should hold copies to allow immediate reference in off-duty hours.

The senior manager for each IT system is responsible for issuing copies of the plans, and for supplying updates to the holders from time to time. All copies of a plan must be subject to change control.

5. Roles and Responsibility

Hospice

This responsibility is delegated as follows: -

Person/Group	Role & Responsibility
SAH Board of Trustees	Ultimate responsibility for the protection of information, in line with the requirements of the GDPR 2018 and Caldicott Principles sits with the Board of Trustees as the Data Controllers. Strategic and Operation responsibility is delegated as below.
Chief Executive	The CE has overall responsibility for ensuring that the governance structures in place for Information Governance and Data Protection are in place and are fit for purpose. This is delegated to the Deputy CEO for strategic and operation development and implementation
Deputy CEO: Head of Clinical Services – (Caldicott Guardian)	• Managing an improvement plan which is monitored through the Information Governance Committee. • Developing protocols for inter-agency information sharing. • Making decisions about how the organisation uses patient identifying information. • Adherence to the Principles of Data Protection as set out in the GDPR 2018; • The Deputy CEO is also responsible for ensuring that should an incident occur, staff have the resources required to manage the situation

Quality and Governance Manager. (Data Protection Officer)	• Chair of the Information Governance Committee • Implementation and monitoring of information security policies, guidelines and procedures. • Auditing current practices and procedures; • Reporting any breaches in Data Protection to the regulatory bodies (ICO and HIS) • Preparing and presenting a report bi- annually to the board of Trustees on any Information Governance Breaches • Operating autonomously to address any issues if they should arise.
Heads of Department	• Ensure there is a process in place to ensure all confidential information is securely stored • Staff and volunteers adhere to this and the related policies in the table above. • Ensuring that confidential information is not disclosed to any unauthorised person.
All Staff and Volunteers	• Ensuring that confidential information relating to patients, visitors, staff, and donors etc. is not disclosed to any unauthorised person and is only utilised for the purpose for which consent has been obtained or for which we have established 'legitimate interest'

N.B. All staff are legally bound to comply with the above. This is re-enforced through their contract of employment (or equivalent formal relationships) with the Hospice. A breach of confidentiality is regarded as serious misconduct. All volunteers are asked to sign a statement of confidentiality on completing induction and failure to maintain confidentiality may result in termination of the volunteer's service

6. Resource Implication

There will be minor financial implications in terms of auditing this policy and planning and implementing any action required to address issues identified.

Minor resources will also be required to communicate the new policy.

Staff training will be provided via current induction opportunities and in line with the needs identified through the PRD/ Appraisal process.

All staff will complete Data Protection training as part of their mandatory training programme which will include Data Protection and Confidentiality awareness. This is a bi-annual training module which will be reviewed through the PRD/appraisal process.

All staff who use IT as part of their role will be required to read and comply with all NHSL Information Security Policies (See Table in No. 2 above)

Information Governance and Data Protection will be covered as part of the robust volunteer induction process.

6. Communication Plan

A copy of all policies & procedures are available in all areas and held centrally on the Policies & Procedures directory on the shared drive. A copy of this policy will be given out as part of induction for new staff, via SMI.

7. Quality Improvement – Monitoring and Review

The Chair of the Information Governance Committee shall ensure that:

- An annual audit is undertaken to review compliance to this policy, and this is discussed at Information Governance meetings
- Any adverse findings in these audits relating to compliance to this policy will prompt the production of a written action plan and a re-audit of the policy.
- Issues relating to consent that are identified as a result of patient surveys are discussed and monitored by the Information Governance Committee when the surveys are published and these will prompt the production of action plans to address issues raised

This policy shall be reviewed no later than two years from the date of issue, or earlier if required in response to any changes in guidance, standards or regulations or as identified through audits to monitor compliance. The Quality & Governance manager is responsible for initiating the review

8. REFERENCES

1. Scottish Executive, National Care Standards – Independent Hospitals. Edinburgh: 2005
2. The Computer Misuse Act (1990)
3. General Data Protection Regulations 2018
4. Human Rights Act 1998;
5. Caldicott Principles; and
6. NHS Scotland Information Security Policy.

Appendix 1

St Andrew's Hospice

Data Subject Access Request

You have the right to ask for copies of your personal data we store and use. This is your right of access, also known as making a subject access request or SAR. We'll normally respond at the latest within one calendar month of receiving your request. There may be times where we need longer or we may need to charge a reasonable fee for admin costs. We'll let you know if this is the case.
You don't have to use this form to ask for copies of your data, but it's helpful for us to know what you're looking for so we can respond fully and promptly.
Please send your completed form to us using the contact details at the bottom of the page.
You can read more about your right of access by visiting: https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/

Who's making this request?

We're asking for your contact details so we can send your response and discuss your request with you (if needed). You only need to give us relevant details. For example, you only need to give us your postal address if you'd like us to respond by post or if you think it would help us identify you. We may ask you for proof of ID if we feel it's reasonable and proportionate. The timescale for responding to your request will start when we receive this.

Your name	Contact number	Email address

Postal address

Are you making this request on behalf of someone else?
☐ Yes
☐ No (Please move to section three)

Please provide contact details of the person you are making the request for.

If you're making the request on behalf of someone else, we need to know who they are and their contact details in case we need to get in touch.

Name of other person | Contact number | Email address

Postal address

Other contact information for the person you are making the request for

You also need to give us proof of your authority to act on their behalf. For example, this could be written authorisation from them or a relevant power of attorney.

Please send proof of authority together with this form when you make your request.
☐ Yes, I've got proof of my authority to act on someone else's behalf and I'll include it with my form. (Please move to section four.)
☐ No, I haven't got any proof of authority yet, but will send it at a later date. I understand you can't action my request until you receive this information.

How would you like us to respond to you?

We'll try and respond to you in the way that suits you. Please let us know if you need us to make any adjustments for you eg large font.
☐ Email ☐ Post ☐ Other (please specify)

What personal data are you requesting?

If you know exactly what personal data you're looking for, it's helpful if you let us know.
For example, if you need a specific email, we could search for this using a particular word or phrase.

Briefly describe your request

Is there a date range of the personal data you're asking for?

It's helpful if you're as specific as possible about your request. For example, if you've been a customer for several years, but you only need data about your recent purchase history, you could ask for data about things you've bought only i the last few months.

Date from | Date to

Can you tell us anything else to help us with our search?

If there's anything else of relevance you can tell us to help us identify you or the data you're requesting, please include this here. For example, any aliases, date o birth, order number or a customer reference number.

Further information to help us find the data you need

Thank you. We'll be in touch. If you'd like more information about how we use your data, please visit www.st-andrews-hospice.com/privacy.