Policy No. 900
Template Ver: Dec 2018

Information Governance Policy	
Originated by:	David Traynier, Head of Quality & Compliance and Data Protection Officer
Date Ratified:	12/2020
Ratified by:	Senior Management Team
Revised by: David Traynier, Head of Quality & Compliance and Data Protection Officer Revision No. 002 Date: 03/2022 Ratified by: Clinical Policies and Procedures Review Group Date ratified: 07/04/2022	
Date of next review: 01/04/2025	
Document Owner:	Data Protection Officer
Document Classification:	Internal

Revision Summary

- 03/2022 Update to Caldicott Guardian section on page 5, to incorporate relevant text from Caldicott Guardian Function Plan [031] and the Caldicott Guardian Role [032], both of which will now be retired.

Revision History

- *08/2021* This is minor update. GDPR has been changed to (UK)(UK)GDPR and there is a short section on transfers to inadequate jurisdictions on page 19.
- *11/2020* This is a new policy, replacing the Information Governance Policy & Procedure [070].

Policy Statement

What is this policy intended to achieve?

The purpose of this policy is the ensure that St Helena has an overall strategy and approach for ensuring good information governance and protecting personal data. It will be supported by related policies relating to specific areas of activity.

To whom does this policy apply?

This policy applies to all St Helena staff, volunteers, and contractors.

Who should read this policy?

This policy may be read by all staff, but all managers should understand and be aware of it, particularly with respect to initiating new processing activities.

Definitions & Terminology

Data Controller – 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law[1]

Data Subject – is an 'identified or identifiable natural person' where that identification is made or made possible, using the data in our possession.[2]

Personal Data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, 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.[3]

Special Category Data – data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data,

[1] (UK)GDPR Article 4(7)

[2] (UK)GDPR Article 4(1).

[3] (UK)GDPR Article 4(1).

biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex like or sexual or orientation.[4]

St Helena's goals are to respect the trust of all those whose personal information we hold, to protect the integrity of that information, and to empower our patients, clients, employees, volunteers, and supporters to manage theirs effectively.

Information Governance (IG) is a framework for handling personal information or data in a confidential and secure manner, meeting appropriate ethical and quality standards.

By handling data securely, St Helena can minimise breaches of IG, which can result in loss of confidence for patients, service users, supporters, staff, volunteers, and other stakeholders, loss of reputation, regulatory sanction, and criminal and civil penalties.

Data breaches fall into one of three categories:[5]

- Confidentiality breach — unauthorised or accidental disclosure of, or access to, personal data.
- Integrity breach — unauthorised or accidental alteration of personal data.
- Availability breach — unauthorised or accidental loss of access, or destruction of, personal data.

When managing personal data, all staff will have regard to the CIA triad: confidentiality, integrity, availability.

The purpose of this policy is to describe the arrangements St Helena has in place to promote and ensure good IG and the context in which that activity occurs. It also explains several key concepts and terms.

[4] (UK)GDPR Article 9(1),

[5] Article 29 Data Protection Working Party Opinion 03/2014, quoted in Article 29 Data Protection Working Party 'Guidelines on Personal data breach notification under Regulation 2016/679,' adopted 3rd October 2017, revised and adopted 6th February 2018.

Key Roles

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is the Director with overall responsibility for information risk at St Helena.

Data Protection Officer

As a public authority under the Freedom of Information Act 2000, St Helena is required to have a Data Protection Officer who is registered by name with the Information Commissioner's Office (ICO). St Helena must also publish on its website a method for the public to contact the DPO.

The DPO will advise on information governance matters across the clinical and non-clinical operations of St Helena, in particular matters relating to the (UK)GDPR, the Privacy and Electronic Communications Regulations (PECR), and the DPA 2018.

The DPO must be facilitated to report to the highest management level of St Helena. In practice, this means that the DPO will produce quarterly IG reports for the Senior Management Team (SMT), via the Director of Care and for the Corporate Governance sub-committee of the Board of Trustees. St Helena will ensure that the DPO receives sufficient training, support and resources in order to fulfil their role and comply with the requirements of (UK)GDPR Article 38. As per Article 38(1), all managers are required to ensure that the DPO 'is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.' All departments must be able to evidence that this advice has been sought and given due regard. Under Article 39, the DPO shall carry out the following task as their minimum obligation:

- Inform and advise the organisation on its obligations under data protection legislation;
- Monitor the organisation's compliance with legislation;
- Provide advice on the conduct of Data Protection Impact Assessments and monitor compliance with them;
- Cooperate with the ICO;
- Act as the point of contact for the ICO on all matters relating to data processing.

As per Article 38(3), SMT and the Board of Trustees will ensure that the DPO does not receive any instruction regarding the exercise of their tasks and are not dismissed or penalised for performing them. The DPO may carry out other tasks, but SMT and the DPO's line manager must ensure that 'any such tasks and duties do not result in a conflict of interests.' In practice,

this would chiefly include operational decision-making about why data is collected or used or information systems procurement.

The DPO will monitor compliance with the (UK)GDPR and other data protection laws, data protection policies, will promote awareness of data protection, will carry out training where needed, and supervise audits.

As well as being an employee of St Helena, the DPO is effectively the representative of the ICO within the organisation, acting as the first line of regulation.

Caldicott Guardian

St Helena is required under Local Authority Circular (LAC 2002/2) to appoint a Caldicott Guardian (and deputy) and ensure they receive appropriate, certified training in their roles. The Caldicott Guardian should be a senior member of the clinical team who will take specific responsibility for protecting the confidentiality and integrity of service users' health and care information. They will also champion patient confidentiality and safe sharing within Patient & Family Services and with SMT and the Board of Trustees. In this, they will cooperate closely with the Data Protection Officer. The specific responsibilities of the role are:

- To ensure PFS always complies with the Caldicott principles.
- To supervise the process for granting patient record access to all external bodies and individuals.
- To promote the safe sharing of patient information when this is necessary to provide high quality care.
- To supervise the publication of the Data Security and Privacy Toolkit self-assessment.
- To work with the Quality & Compliance Department to maintain an up to date and accurate Record of Processing Activities for PFS.
- To work with the Quality & Compliance Department to maintain an up to date and accurate Information Asset Register for PFS.
- To ensure that patient confidentiality is a principal consideration in all PFS projects, initiatives, and organisational developments, in line with the principle of data protection by design and by default (see page 8).
- To ensure all PFS staff receive adequate and appropriate confidentiality training.
- To chair the Records Management Group.

- To approve all PFS policies and procedures concerning records management and the handling of patient identifiable data.
- To raise concerns with the Data Protection Officer and Senior Information Risk Officer, as appropriate.
- To report on matters concerning patient confidentiality and records management to the Board of Trustees.
- To liaise with external providers on patient confidentiality matters.
- To ensure that the details of the Guardian and Deputy Guardian are registered with NHS Digital.

At St Helena, the Caldicott Guardian is the Director of Care and the Deputy is the Medical Director. For more detail on the Caldicott Principles, see Page 17.

Training

SMT will ensure that the Caldicott Guardian and Deputy received accredited training upon recruitment, to be refreshed every three years.

Legislative framework

To be fully compliant, St Helena must have an accurate and current understanding of the legislative and regulatory environments in which it operates. This understanding has two prerequisites.

The first prerequisite is that St Helena must comply with the General Data Protection Regulation ((UK)GDPR) as enacted by the Data Protection Act 2018, which apply to the entire organisation. It will be the responsibility of the Data Protection Officer to interpret the legislation and advise managers and staff on its correct application to all St Helena operations. The DPO should aim to strike the correct balance between protecting data subject rights, on the one hand, and not needlessly impeding St Helena's activities, on the other.

The second prerequisite is that individual service leads must be aware of the regulatory requirements and codes of practice that govern their area of operation. These cannot reduce the minimum standards required by data protection legislation, but they may impose additional or higher requirements in some areas. Sources of additional regulation would include, the Care Quality Commission, the Gambling Commission, the Charity Commission, and the Fundraising Regulator.

Data protection principles

There are six data protection principles laid out in the (UK)GDPR[6] These are that personal data should be;

- used fairly, lawfully and transparently.
- used for specified, explicit purposes.
- used in a way that is adequate, relevant and limited to only what is necessary.
- accurate and, where necessary, kept up to date.
- kept for no longer than is necessary.
- handled in a way that ensures appropriate security, including protection. against unlawful or unauthorised processing, access, loss, destruction or damage.

In addition, the (UK)GDPR (5)(2) specifies that St Helena 'shall be responsible for, and be able to demonstrate compliance' with, these principles. In other words, the burden of proof lies with St Helena to demonstrate we are compliant and not with our regulators to demonstrate that we are not.

At St Helena, the Data Protection Officer advises and informs on proper compliance with the (UK)GDPR and the DPA2018; however, responsibility for compliance remains with line managers. All projects that propose the novel collection, use or sharing of personal data must be referred to the DPO in a timely way to ensure they are properly assessed for compliance before they commence.

All processing activities (new or existing) must be registered in the St Helena Record of Processing Activities (ROPA) on the Sentinel system. For advice, consult the Data Protection Officer or the Compliance Officer.

Governance Model

St Helena operates a hybrid governance model. This comprises two distinct components.

The Quality & Compliance Department is a hub for providing support and advice to other departments. It also monitors compliance across the organisation and reports upward to the Senior Management Team and the Trustee subcommittees.

[6] (UK)GDPR Article 5.

Each service area will have a designated governance lead who will be the first point of contact for Quality & Compliance staff. This governance lead will work with DPO to manage IG issues and provide early notice of concerns and incidents.

Privacy Maturity Model

St Helena will employ the AICPA/CICA[7] Privacy Maturity Model (PMM) to evaluate the quality of its information governance processes. It will be the responsibility of department heads to monitor the maturity of their own processes (with support from the Quality & Compliance Department) and to report concerns upward.

The PMM uses five maturity levels to evaluate internal processes.

1. *Ad hoc.* Procedures or processes are generally informal, incomplete, and inconsistently applied.
2. *Repeatable.* Procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects.
3. *Defined.* Privacy procedures and processes are fully documented and implemented, and cover all relevant aspects.
4. *Managed.* Reviews are conducted to assess the effectiveness of the privacy controls in place.
5. *Optimised.* Regular review and feedback are used to ensure continuous improvement towards optimization of privacy processes.

Data Protection by Design and Default

As required by (UK)GDPR Article 25, St Helena will ensure data protection by design and by default.

Data protection by design[8] is the principle that data protection and privacy will be considered at the time new processes, projects, services, products, or systems are designed, not afterward. It also means that data protection must be considered at all points of the lifecycle.

---

[7] American Institute of Certified Public Accountants and the Canadian Institute of Accountants.

[8] Also known as 'Privacy by Design'. This is to be done considering 'the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying

Data protection by default derives from the data protection principles of data minimisation and purpose limitation. It means that new systems and processes collect only the minimum information to fulfil their purpose and that where something can be kept private, by default, it is kept private.

In practice, adhering to both principles means that data protection considerations should be considered when a project is begun and not as it nears completion. Service leads must proactively consult with the Data Protection Officer before all novel uses of personal data or developing new processes and services.

Data Protection Impact Assessments

A Data Protection Impact Assessments (DPIAs) is a process for identifying and minimising the data protection risks of a processing activity. St Helena must undertake a DPIA for any activity that is likely to result in a high risk to individuals. DPIAs should be considered for any large scale processing, systematic monitoring, processing of sensitive or highly personal data, evaluation or scoring, or novel use of technology.

A DPIA must be undertaken in situations including (but not limited to) those where the objective is:

- The systematic and extensive profiling or automated decision-making to make significant decisions about people;
- To process special-category data or criminal-offence data on a large scale;
- To systematically monitor a publicly accessible place on a large scale;
- To use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
- To combine, compare or match data from multiple sources;
- To process personal data in a way that involves tracking individuals' online or offline location or behaviour.

---

likelihood and severity for rights and freedoms of natural persons posed by the processing' ((UK)GDPR Article 25(1)).

- To process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them[9]

As a rule, before embarking on a new processing activity, the lead responsible for the activity should consult with the DPO so that, if necessary, a DPIA can be carried out before work commences. It is not acceptable to begin a project and then carry out the DPIA.

DPIAs should be logged on the DPIA Sentinel module. DPIAs should comply with the latest ICO guidance and the requirements laid out in 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.'[10] While the DPO can advise and assist, responsibility for carrying out a DPIA remains with the project lead or manager. DPIAs should be regularly reviewed and updated.

Information Security

St Helena will comply with (UK)GDPR Article 32 to ensure security of processing by implementing appropriate technical and organisational measures that consider 'the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons…' These measures may include but are not limited to:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; for example, by means of electronic encryption, password protection, electronic and physical access control, and activity logging;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

[9] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-(UK)GDPR/accountability-and-governance/data-protection-impact-assessments/

[10] Article 29 Data Protection Working Party WP 248 rev.01 as last Revised and Adopted on 4 October 2017.

- The secure destruction of electronic and hardcopy data and data sanitisation of electronic devices according to standards devised by the IT Department.

These measures will be assured through appropriate system level security and information technology policies and procedures and business continuity plans.

Information Asset Register

St Helena will also maintain an Information Asset Register and carry out periodic information flow-mapping. Technical measures will be the responsibility of the Head of IT with wider organisational measures to be supervised by the DPO.

Each entry on the Information Asset Register must be assigned an owner, and these owners will be responsible for ensuring that assets are correctly classified according to their security needs according to the following classification scheme.[11]

- Confidential (only senior management have access)
- Clinical confidential (only accessible to Registered Healthcare professional or staff operating under their authority while providing patient care)
- Restricted (most employees have access)
- Internal (all employees have access)
- Public information (everyone has access)

St Helena will further ensure that any person acting under its authority who has access to personal data will act in a way that respects the data's confidentiality and integrity. St Helena will ensure this through appropriate use of confidentiality agreements, IG training, and audit and monitoring.

Information Asset Owners will have due regard to correctly valuing the information assets that are their responsibility. This can be done by considering the following questions:

- The original cost of producing the information;
- The value of the information if sold on the open market;
- The cost to St Helena of reproducing the information;

[11] This is adapted from ISO 27001:2013.

- The degree to which the information makes organisational/departmental objectives feasible;
- The consequences should the information become unavailable;
- The advantages to a competitor if they could use, change or destroy the information;
- Our likely financial liability (compensation claims, fines) should the information be subject to unauthorized release, destruction or alteration;
- Reputational damage and loss of public/patient confidence in St Helena.

The Quality & Compliance Department will enforce compliance with a schedule of periodic reviews.

Record of Processing Activities

St Helena is required under Article 30 of the (UK)GDPR to main a record of all activities involving the processing of personal data. In this context processing means anything done to or with data, including storage. Article 30(1) (a-g) requires at a minimum that the record include:

- The name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer.
- The purposes of the processing.
- A description of the categories of data subjects and of the categories of personal data.
- The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations.
- Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, where appropriate, the safeguards applied.
- Where possible, the envisaged time limits for erasure of the different categories of data.
- A general description of the technical and organisational security measures used to protect the data.

St Helena will maintain a Record of Processing Activities (ROPA) using a dedicated module of the Sentinel system. It will be the responsibility of each service area, with support from the Quality & Compliance Department, to maintain an accurate and up to date ROPA. The Quality & Compliance Department will enforce compliance with a schedule of periodic reviews.

Training and Education

All St Helena staff will be given mandatory training on induction on the following My Learning Cloud modules:

- Protecting Personal Information.
- Document and Record Keeping.

Staff will also receive refreshers on both modules. For PPI, the refresher will be annual. For DRK, the period will be every three years. Staff may also be required to retake these modules at the discretion of their line managers; for example, following an IG incident.

The Human Resources Directorate will supply the DPO with monthly compliance figures for upward reporting.

Incident reporting

(UK)GDPR (4(12)) defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

St Helena is required, under Article 33 of the (UK)GDPR, to maintain a record of all personal data breaches, however minor. All IG incidents must therefore be logged on Sentinel, including those that do not involve personal data. Significant attempts to breach either network or physical security should also be reported as incidents. All breaches will be dealt with by the appropriate line manager but will also be notified automatically to the DPO who will provide advice and support.

Article 33 of the (UK)GDPR requires St Helena to report personal data breaches to the ICO within 72 hours of us becoming aware of them (irrespective if weekends) unless they are unlikely to risk the rights and freedoms of the affect individuals. Failure to report may leave St Helena liable to a substantial fine.[12] It is for this reason that that internal standard for reporting is stringent: staff must report IG incidents immediately, certainly within 24hrs. There are no exceptions. This is to allow managers and the DPO sufficient time to assess whether the breach should be reported to ICO. Reporting to the ICO shall be the responsibility of the DPO.

[12] The maximum fine that can be levied for an administrative breach of this nature is €10,000,000 or 2% of gross annual turnover, whichever is the higher.

Notifiable non-clinical incidents should be reported directly to the ICO using their online form. Notifiable clinical incidents should be reported using the tool provided in the Data Security and Protection Toolkit. If the incident meets a certain threshold, then this system will forward the details to NHS Digital, the Department of Health and Social Care (DHSC), the ICO, and other regulators.[13] It is not necessary to report an incident to NHS Digital and the ICO separately.

The DPO will produce a monthly digest of IG incidents for the Senior Management Team. For detailed guidance on reporting IG incidents, refer to the appropriate section of the Clinical Incident Management Policy [013].

Records Management and Data Retention

St Helena will comply with the fifth data protection principle by ensuring that data, in particular personal data, is not kept any longer than is necessary. To accomplish this, all St Helena staff will adhere to their departmental data retention policies and accompanying retention schedules.

It is the responsibility of managers and service leads to ensure that these schedules are kept up to date. The Patient and Family Services directorate will also adhere to the Records Management Policy [105]. Each service/department will conduct quarterly data retention audits using an approved template and provide these results to the Quality & Compliance Department for upward reporting.

Rights of the Data Subject

Under the (UK)GDPR Articles 12-23, anyone whose personal data we process has rights in respect to that data. These rights are:

The right to be informed.

- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability

[13] NHS Digital 'Guide to the Notification of Data Security and Protection Incidents,' September 2018 Health and Social Care Information Centre, p. 7.

- Right to object
- Rights relating to automated individual decision-making, including profiling.

None of these rights is absolute, but St Helena has a duty to facilitate any data subject's rights, primarily through timely response to data subject access requests. The right to be informed must be met first and foremost through the maintenance of publication of an adequate privacy notice, which must be available to data subjects at the point we collect data from them or on request. The remaining rights will be managed on a case-by-case basis following the procedure laid out in the Data Subject Request Policy [902]. All DSARS will be managed on the appropriate Sentinel module.

Measuring Compliance

Audit

Each department will be required to conduct periodic IG audits as appropriate. These audits will be supported by the Quality & Compliance Department. Examples of such audits include:

- Departmental walkrounds.
- Document retention on network drives and SharePoint folders.
- Quality of Data Subject Access Request responses.
- Quality of Processing Activity records.
- Destruction of records.
- Destruction of equipment.

Metrics

A data protection metric is a tool for facilitating decision making and accountability throughout St Helena. Metrics must be measurable, meaningful, clearly defined, and specific. Metrics can be set centrally or locally. All metrics must have an owner and be established according to an organisationally approved template.

The DPO will supervise reporting of the following data protection metrics to operational management and the Senior Management Team. Directors shall be responsible for reporting to the appropriate Trustee subcommittees.

- An up to date and adequate organisational privacy notice
- No. of Data Subject Access Requests (DSARS)

- DSAR response compliance
- Compliance with the Data Retention Policy
- No. of Information Governance Incidents, complaints, and breaches
- Mandatory training compliance
- No. of Data Privacy Impact Assessments
- Record of Processing Activities Compliance

Contracts, Partnerships, and Relationships with Third Parties

Where St Helena or individual services enter contracts and arrangements with third parties, it is the responsibility of the relevant manager to consider any data processing arrangements that will exist between the parties. Before committing to any agreements or signing any contracts, a due diligence assessment must be documented, to assure St Helena that the potential partner is a reputable and reliable data processor. The DPO can advise on the nature of the checks to be carried out.

Managers must also ensure that any contract incorporates an adequate Information Sharing Agreement that conforms with the requirements laid out in (UK)GDPR Article 28. These agreements must be included in the relevant entry on the ROPA. For further information on this, see the Contract Management Policy [912].

Information governance and clinical services

St Helena's lawful basis under the (UK)GDPR for processing personal data is Article 6(1)(e), that 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.' To the extent that it provides clinical services, St Helena is a public authority, as defined in the Freedom of Information Act 2000.[14] The statutory authority for St Helena's processing information as a public authority is the duty imposed upon us, under Section 251B of the Health and Social Care (Quality and Safety) Act 2015, to share information where this may be likely to facilitate the provision to the individual of health services or adult social care in England and is in the individual's best interests.

[14] Note that St Helena cannot be regarded as a public authority in respect to any of its other activities, such as employment of staff, retail, or lottery.

As the healthcare data we process is regarded as special category data, St Helena requires a second lawful basis specifically for processing this type of sensitive data. The lawful basis for this is Article 9(2)(h) of the (UK)GDPR '…the provision of health or social care or treatment or the management of health or social care systems…'

Openness

St Helena recognises, with respect to its clinical operations, that it has a responsibility to find an appropriate balance between confidentiality and openness in the management of personal information. In particular, we note the 2013 Caldicott review, which added a seventh principle, that 'Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by' the other principles.[15] It is not acceptable if the care a patient or service user receives is undermined because different organisations involved in that care did not share information effectively. St Helena will therefore abide by the seventh principle, 'duty to share information can be as important as the duty to protect patient confidentiality.'

Caldicott principles

In addition to the (UK)GDPR, St Helena must also take note of the Caldicott principles. The original six Caldicott Principles were developed in 1997, with a seventh added in 2013. At St Helena, the Caldicott Guardian is entrusted with ensuring that these principles are observed by all staff.

Principle 1 - Justify the purpose(s) for using confidential information

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 - Use the minimum necessary personal confidential data

[15] Department of Health (2013) 'The Information Governance Review,' p. 21

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 - Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The Caldicott principles complement those specified by the (UK)GDPR; however, for the avoidance of doubt, the (UK)GDPR takes legal precedence. Any perceived conflicts should be referred to the Data Protection Officer or the Caldicott Guardian for clarification.

Any incidents related to the security of patient information must be reported with 24 hours to the Caldicott Guardian using the incident reporting system. An incident may include the loss,

authorised disclosure, unauthorised amendment, insecure transmission, or deletion of a health record. For more detail, see the Incident Management Policy [013].

Records Management Group

Matters pertaining to the management of clinical records will be supervised by the Records Management Group, which shall be chaired by the Caldicott Guardian. The primary policy covering records management functions is the Records Management Policy [105].

Data Security and Protection Toolkit

St Helena is required to complete an annual self-assessment using the Data Security and Protection Toolkit (DSPT) to assure compliance with the Data security and Protection Standards for Health and Care.[16] Each assessment must be submitted online by no later than 31st March. The self-assessment will be managed by the Head of Quality & Compliance, who will designate leads as appropriate for assessing and assuring compliance with each of the assertions covered by the Toolkit. Where compliance cannot be assured, Head of Quality & Compliance will work with the relevant lead to develop an action plan.

Summarised results of this self-assessment will be made available via the NHS Digital website and St Helena will also publish the resulting rating in its annual Quality Account and share it with the Care Quality Commission via the next available Quarterly Quality Report.

Associated Policies and Procedures

- Records Management Policy [105]
- Acceptable Use Policy [400]
- Network Security Policy [411]
- Information Classification Policy [908]
- Contract Management Policy [912]
- Incident Management Policy [113]

[16] Known until 2018 as the Information Governance Toolkit.

Compliance with Statutory Requirements

- Data Protection Act 2018
- General Data Protection Regulation (Regulation (EU) 2016/679)
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003

Responsibilities/Accountabilities

Title	Accountability
Chief Executive Officer	Responsible for ensuring overall compliance with this policy.
Senior Information Risk Owner	Overall ownership of St Helena's information risk management and data protection strategy.
Caldicott Guardian	Senior clinician, responsible for ensuring confidential patient information is used securely and shared effectively.
Data Protection Officer	Non-executive officer tasked with monitoring and promoting overall compliance with data protection legislation and good practice.
Directors	Responsible for ensuring compliance with this policy within this directorate and ensuring the Quality & Compliance Department has a point of contact and support.
Quality & Compliance Department	Responsible for managing, administrating, and reporting on compliance with this policy.
IT Department	Responsible for ensuring St Helena employs all reasonable technical measures to ensure the security and confidentiality of data.

Staff Training Requirements

All staff will carry out Information Governance training on induction using My Learning Cloud, followed by annual refreshers. The DPO will provide ad hoc and additional training as required.

Monitoring (Including Audit) and Frequency of Review

The DPO will monitor compliance with this policy and report quarterly to the Senior Management Team and the Corporate Governance Committee. This policy will be reviewed routinely every three years.

Data Protection

Does this Policy require sign off from the Data Protection Officer?	Yes	
DPO approved: David Traynier		Date: 01/12/2020
DPO comments	This policy was written by the Data Protection Officer.	

References:

NHS Digital ‘Guide to the Notification of Data Security and Protection Incidents,’ September 2018 Health and Social Care Information Centre

Equality Impact Assessment Initial Screening Tool

Document Reviewer(s):	David Traynier, Head of Quality & Compliance	Date Assessment Completed:	25/11/2020

Assessment of possible adverse impact against any minority group			
Could the document have a significant negative impact on equality in relation to each area below?	Response		If yes, please state why, and the evidence used in your assessment
	Yes	No	
1. Age		X	
2. Sex		X	
3. Disability		X	
4. Race or Ethnicity?		X	
5. Religion and Belief?		X	
6. Sexual Orientation?		X	
7. Pregnancy and Maternity?		X	
8. Gender Reassignment?		X	
9. Marriage and Civil Partnership?		X	

- You need to ask yourself:
- Will the document create any problems or barriers to any community or group?
- Will any group be excluded because of this document?
- If the answer to either of these questions is yes, you must complete a full Equality Impact Assessment.

Assessment of positive impact			
Could the document have a significant positive impact by reducing inequalities that already exist?	Response		If yes, please state why, and the evidence used in your assessment
	Yes	No	
1. Promote equal opportunities		X	

2. Eliminate discrimination		X	
3. Eliminate harassment		X	
4. Promote positive attitudes towards disabled people		X	
5. Encourage participation by disabled people		X	
6. Consider more favourable treatment of disabled people		X	
7. Promote and protect human rights	x		This document will help promote data subject rights and the right to privacy.

On the basis of the information/evidence/consideration so far, do you believe that the document will have a positive or negative adverse impact on equality?

Positive	Please rate (delete as applicable) the level of impact					Negative
		LOW				

Is a full equality impact assessment required? No