Woking & Sam Beare
Hospice and Wellbeing Care

`

INFORMATION GOVERNANCE POLICY

Policy / procedure code:	IG01
Version:	V2
Policy owner:	SIRO
Approval Date:	25/06/2021
Ratified by:	Governance Committee
Next Review Date:	June 2024
For Information and action to:	All staff and volunteers

Version Control Sheet

Policy / Procedure: Information Governance Policy

Version	Date	Author	Status	Comment
V1	July 2015	B Hamilton	Approved	
V1.1	July 2016	B Hamilton	Approved	Revised with addition of Data Flow Maps
V1.2	Oct 2017	B Hamilton	Approved	Review / Proposed GDPR changes required
V2	May 2021	J Gardner	Approved	Full review and update carried out by IG Leads, SIRO, IT Manager, Caldicott Guardian and CEO.

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version on the R Drive is the controlled copy. Any printed copies of this document are not controlled. As a controlled document this document should not be saved onto another Drive and should only be accessed from the R Drive: R:\Policies and Procedures\POLICIES & GUIDELINES\Information Governance

Contents **Page**

1. Introduction

Information Governance (IG) is a framework for handling personal information in a confidential and secure manner that meets the required standards and legislation. It provides a consistent way to manage many different information handling requirements including:

- Information Governance Management
- Clinical Information assurance for safe patient care
- Confidentiality and Data Protection assurance
- Corporate Information assurance
- Respecting data subjects' rights regarding the processing of their personal data

2. Purpose

The purpose of this policy is to describe the systems and processes that ensure WSBH meets its responsibilities for the management of information assets and resources which ensures information is:

- Held securely and confidentially
- Processed fairly and lawfully
- Obtained for specific purpose(s)
- Recorded accurately and reliably
- Used effectively and ethically
- Shared and disclosed appropriately and lawfully

This policy is the central policy in a suite of policies that:

- Informs staff how they should use and protect information appropriately according to the Caldicott Principles
- Ensures the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.
- Ensures technology is secure and up to date

This Policy should be read in conjunction with all relevant policies, processes, standard operating procedures (SOPs) and guidance that cover the use and security of information, (Appendix 1).

3. Scope

This Policy applies to all information obtained and processed within the Hospice held electronically, in manual paper-based filing systems and in other formats, relating, but not limited to:

- Patient / client / service user, customer information
- Employee and personal information

- Organisational business and operational information
- Clinical research, audit and reporting information
- Commercial and contract details

This policy applies to:

- Employed staff (including Bank staff and staff on fixed or temporary contracts)
- Volunteers
- Staff placements (students, medical staff and allied healthcare professionals)
- Locums
- Agency staff

4. Legal and Compliance Standards

WSBH is required to ensure that relevant UK legislation and standards are understood and that the Hospice can demonstrate compliance.

4.1 Key Legislation and Guidance

WSBH must ensure that all policies and procedures are compliant with legislation and relevant NHS guidance on the management of information, including but not limited to the following:

- The UK General Data Protection Regulation (GDPR)
- The Data Protection Act 2018 (DPA 2018)
- Common Law Duty of Confidentiality
- The Eight Caldicott Principles (2020)
- National Health Service Act (2006)
- Health and Social Care Act (2012)
- The Health and Social Care (Safety and Quality) Act (2015)
- Health and Social Care (National Data Guardian) Act (2018)
- Human Rights Act (1998)
- Computer Misuse Act (1990)

4.2 The Data Security and Protection Toolkit

The Data Security and Protection Toolkit (DSPT) is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards (Appendix 2).

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

WSBH is required to submit the online self-assessment by the deadline set by NHS Digital annually.

5. Roles and Responsibilities

Under the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 and the Data Security and Protection Toolkit the WSBH is required to demonstrate that it has an Information Governance Framework supported by the following roles:

Management Structure and Responsibilities	
Roles	**Responsibilities**
Board	• Accountable for WSBH delivering the Information Governance Agenda and ensuring data protection legislation and the Data Security and Protections Toolkit compliance.
Chief Executive	• Delegated overall accountability for Information Governance and compliance with the applicable legislation and regulations
Governance Committee	• Provides assurance to the Board and manages the relevant risks and issues that are escalated by the Management Team.
Management Team	• Set the Information Governance strategy and ensure it is translated into an effective organisational management plan with sufficient resources and monitoring. • IG Policy • Ensure compliance and sign off of the Data Security and Protection Toolkit providing assurance of meeting key requirements and robust improvement plans are in place to address any shortfalls • Ensure that information risks are assessed and mitigated to an acceptable level and handled in a similar manner to other major risks such as financial, legal and reputational risks • Review serious incidents involving actual or potential loss of personal data or breach of confidentiality which must be published in annual reports and to the Information Commissioner
Senior Information Risk Owner (SIRO)	• Responsible for the Hospice’s compliance with Information Governance Management and will advise the Board on the effectiveness of information risk management and risk issues • Authorises the submission of the Data Protection and Security Toolkit
Caldicott Guardian	• Protects the confidentiality of patient and service user information and enables appropriate information sharing • Champions IG requirements and issues at the Board and Management Team meetings
IG Leads / IT Manager	• Oversees the IG requirements for WSBH and ensures appropriate systems and processes are in place to support adherence to standards • Leads the delivery of the IG Improvement Plan • Completes the allocated components of the DSPT within the required timeline for the annual assessment

	- In support of the SIRO ensures that Information Asset Owners (IAOs) are nominated to manage local responsibilities and confidentiality within their work area.
Information Asset Owners	- Accountable to the SIRO for providing assurance on the security and use of the information assets within their respective area are identified, recorded and controls are in place to mitigate any risks.
Managers	- Ensure policy standards and guidelines are built into local processes to secure compliance - Ensure all job descriptions contain the relevant responsibility for information security, confidentiality and records managements - Ensure staff undertake IG mandatory training - Ensure any data protection incident is reported and investigated appropriately and escalated in the event of a serious incident.
Staff (as defined in the Scope)	- Must adhere to this Policy and all associated IG policies and procedures. - Mandated to undertake IG Training
3rd Party contractors	- Appropriate contracts that meet UK GDPR requirements to guarantee appropriate technical and organisational measures are in place that protect data subjects' rights for any service provider with potential or actual access to identified information assets.

Note: Under the UK GDPR WSBH is not required to appoint a Data Protection Officer as the type of organisation and scale of processing does not meet the definitions but is required to achieve its data protection obligations through sufficient staff and resources.

6. Key Tasks

Information Governance Management covers all IG compliance and operational requirements. Specific key Information Governance Management work areas are outlined below but the subsidiary supporting policies, processes and guidance should be referred to for more detail.

6.1. Data Protection Impact Assessments

A Data Protection Impact Assessment must be completed whenever there is a change that is likely to involve a new use or significant change the way in which personal data is processed to identify and minimise the data protection risk.

Staff involved in procurements of new systems, setting up new services or ways of working are responsible for ensuring the IG Lead is involved in the project plan. The Privacy Impact Assessment Policy and assessment template are saved on the R Drive.

6.2. Data Sharing

WSBH will share personal data with other organisations where there is a lawful basis to do so i.e. for the provision of direct care and treatment of individuals.

A Data Sharing Agreement (DSA) is required when any data is shared between the Hospice and another organisation that is **not** for the purpose of direct patient care. A DSA will set out the purpose and detail of what will be shared, including how it will be transferred securely and to whom.

6.3. Data Retention

Records will be stored securely for the appropriate length of time in accordance with the Records Management NHS Code of Practice for Health & Social Care 2016 for clinical records and the Corporate Records Retention and Disposal Schedule for non-clinical records.

6.4. National Data Opt Out

The national data opt-out was introduced on 25 May 2018 and enables patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian.

WSBH does not share patient personal data with other organisations for secondary uses and would only use patient data with consent for the purposes of research as set out in the Privacy Notice and Patient Information leaflet 'Your information, why we need your data and how it is used'.

6.5. Information Flow Mapping

The IG Lead is responsible for ensuring appropriate information flow maps are in place for WSBH IT systems and operational services.

6.6. Incident Reporting

The WSBH Notification of Data Security and Protection Incidents Policy sets out the process for all IG incidents or near misses to be recorded on the Hospice's Incident reporting system, Sentinel. This provides the mechanism for incidents to be monitored, managed, investigated and lessons learned.

The Governance Committee (quarterly) receives reports on incidents, complaints and near misses. Under data protection legislation serious incidents must be reported to the ICO within 72 hours. All serious incidents will be reported to the Management Team and Board by exception reporting.

6.7. Information Governance Audit

The IG Lead will complete a Data Protection and Security Audit annually or more frequently in response to a serious incident or trend.

6.8. Subject Access Requests

Subject Access Requests (SAR) are registered by the Quality Assurance Manager and processed with guidance from the Caldicott Guardian by the appropriate member(s) of staff within the required timeline as set out in the Subject Access Request Framework.

6.9. Freedom of Information Requests

The Freedom of Information Act does not apply directly to WSBH, as a non-public authority, but the organisation may be required to assist an NHS public body with a request under contractual obligation.

6.10. Advice and Guidance

The IG Lead and Caldicott Guardian will provide subject matter advice when required.

6.11. Information Asset Management

The IT Team will maintain the Hospice's IT Asset Register and Data and Purpose Log.

6.12. Information Governance and Security Incident Management

All IG incidents will be reported on the Hospice's reporting system, (Sentinel), in accordance with the Notification of Data Security and Protection Incidents Policy.

6.13. Training

Mandatory IG training for all staff is included in the Hospice's statutory and mandatory training requirements. Training compliance is monitored and reported to the Governance Committee.

7. Monitoring

Compliance with this policy will be monitored via the Governance Committee. This policy will be subject to audit by the Management Team.

This policy will be reviewed three yearly or more frequently in accordance with legislation or national guidance changes.

8. Equality Impact Assessment

WSBH is committed to creating a positive culture for all staff and service users.

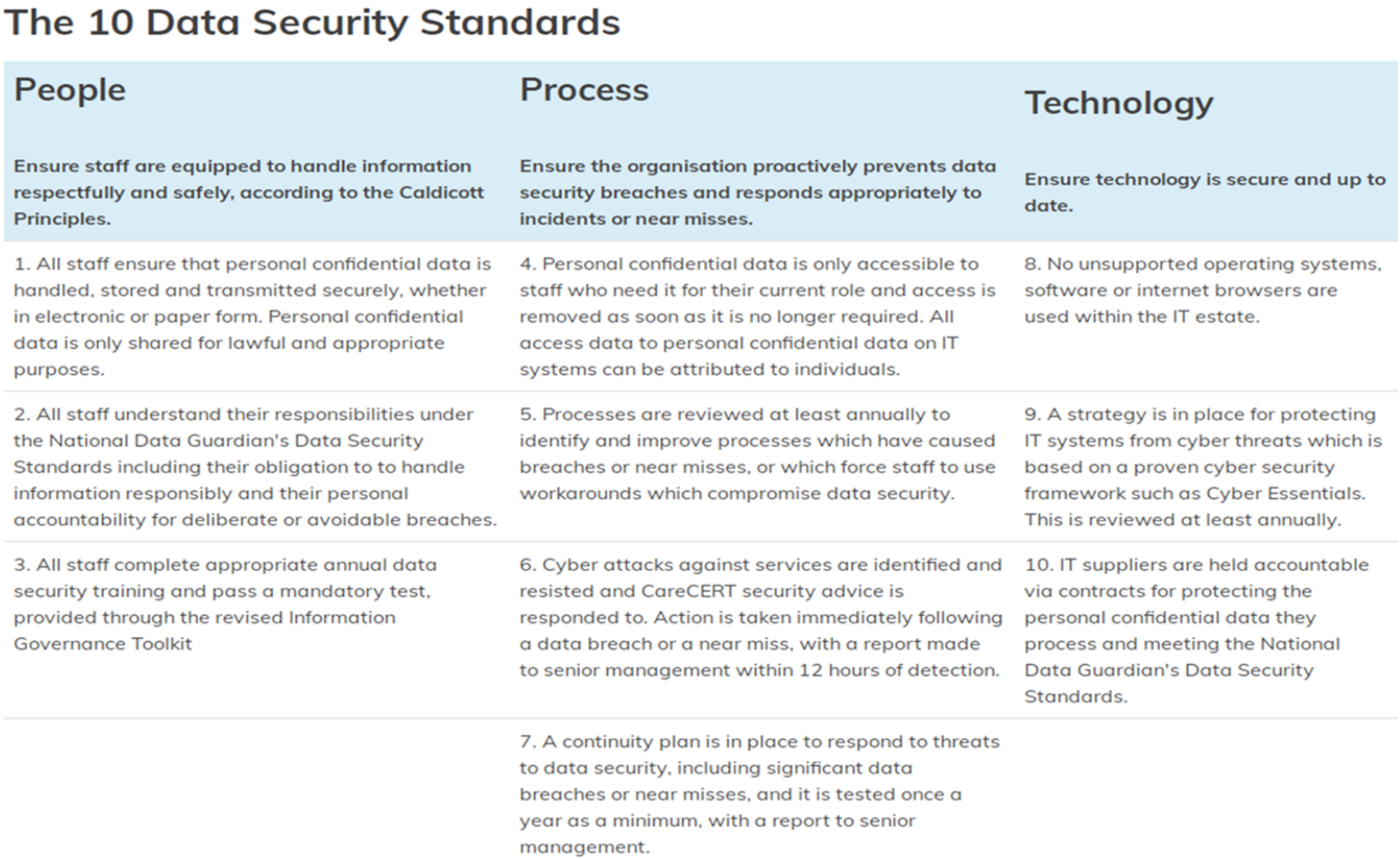
The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment, pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

PROTECTED CHARACTERISTIC	EQUALITY IMPACT ASSESSMENT
Age	There is no evidence to indicate that any staff member or volunteer represented in these Protected Characteristic groups is, as a result of this Policy, affected more or less favourably than staff and volunteers in other groups
Gender	
Gender Re-assignment	
Sexual Orientation	
Race	
Religion or Belief	
Marriage / Civil Partnership	
Pregnancy / Maternity	
Disability	

Appendix 1: Relevant WSBH Information Governance Policies

- ICT001 Information Security Policy
- ICT002 Mobile and Remote Access Policy
- IG02 Data Protection and Confidentiality Policy
- IG03 Data Quality Policy
- IG04 Clinical Records Management
- IG05 Organisational Change Policy
- IG06 Privacy Impact Assessment Policy
- IG07 Clinical Subject Access Requests Framework
- IG08 Notification of Data Security and Protection Incidents Policy

Appendix 2



The 10 Data Security Standards

People	Process	Technology
Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.	**Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.**	**Ensure technology is secure and up to date.**
1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.	4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access data to personal confidential data on IT systems can be attributed to individuals.	8. No unsupported operating systems, software or internet browsers are used within the IT estate.
2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to to handle information responsibly and their personal accountability for deliberate or avoidable breaches.	5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.	9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit	6. Cyber attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.	10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.
	7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.	