INFORMATION GOVERNANCE POLICY

WESTON HOSPICECARE GROUP OF COMPANIES

POLICY APPROVAL, RATIFICATION & SIGNATURE		
Policy Author	**John Bailey, Director of Patient Services & John Bangham, Project Finance Director**	
Date of first issue	**3rd August 2017**	
This version no. Date of issue	**Version 4 20th February 2020**	
Approved by:  **Paul Winspear Chief Executive**		**Ratified by:**  **Judi Driscoll Chair of Board of Trustees**
Next review date	**20th February 2021**	
Document location	**F:\EVERYONE\Policies & Procedures**	

Document Control

Printed copies of this policy are uncontrolled. Validity of content is only assured by referring to the most current live document on the hospice server.

Equality and Diversity

Weston Hospicecare is an equal opportunities employer and does not discriminate on the grounds of age, disability, gender, maternity and pregnancy, race, religion, or sexual orientation. When implementing this policy, all staff must ensure compliance with the Equalities Act 2010.

Summary

This policy sets out the overall framework for managing all information including data at Weston Hospicecare, in accordance with relevant legislation and best practices nationally. Information may be stored both physically and digitally.

"Hospice" is used herein to refer to the organisation comprised of the Weston Hospicecare group of companies.

1. Scope

This policy applies to all staff, employees and volunteers, in the service of Weston Hospicecare and covers all our activities, information systems, networks and physical environment.

2. Purpose

Information is a vital asset, both in terms of the clinical management of patients and the efficient management of Hospice services and resources. It plays a key part in Hospice governance, service planning and performance management.

It is therefore of paramount importance to ensure that all information is efficiently managed, with appropriate policies and procedures, management accountability, and working structures to provide a robust governance framework for information management, particularly with regard to personal data and confidential/sensitive information such as patient and staff personal data. This Information Governance (IG) Policy sets out how the Hospice shall achieve these aims, to manage information legally, securely, efficiently, effectively and appropriately with respect to;

- All information used by the Hospice in the course of discharging its duties and obligations;
- All information systems managed by the Hospice;
- Any individual or organisation, including third parties, with access to information used by the Hospice.

Personally Identifiable Data (PID) includes, but is not limited to, patient information, staff (employees and volunteers) information and donor/supporter information. PID is any information that can be used directly, or in combination with other sources of information, to uniquely identify, contact or locate a single person, and is thus considered privileged and confidential.

3. Principles

Health care professionals should have the confidence to share information in the best interests of their patients/service users within the framework set out by the Caldicott Principles.
Every data information asset (piece of information) used by the Hospice must be justifiable and accountable in terms of why it is required, how it is acquired, how it is used, with whom it is shared, how it is stored, who has access to it, and how long it is retained. Data information assets may be in either digital form (softcopy) or physical form (hardcopy).

There are four key interlinked strands to the IG Policy:

- Openness
- Legal compliance
- Information security
- Quality assurance

	Appendix 1
Openness	
• Non-confidential information on the Hospice and its services should be available to the public through a variety of media.	A, I
• Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients.	D, E, C
• The Hospice will have clear procedures and arrangements for liaison with the press and broadcasting media.	I
• The Hospice will have clear procedures and arrangements for handling queries from patients and the public.	C, D, E
Legal Compliance	
• The Hospice regards all identifiable personal information relating to patients as confidential.	B, E
• The Hospice regards all identifiable personal information relating to staff and donors/supporters as confidential except where regulatory requirements pertaining to accountability and openness require otherwise.	
• The Hospice will establish and maintain policies to ensure a responsible attitude towards key legislation, including but not limited to;	M, E
○ Data Protection Act 2018	
○ Human Rights Act 1998	
○ General Data Protection Regulations 2018	
○ Common Law Duty of Confidentiality	
• The Hospice will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation, e.g. Health and Social Care Act 2012, Crime and Disorder Act 1998, Protection of Children Act 1999.	M, O
• The Hospice will carry out a Data Protection Impact Assessment prior to new services or new information processing/sharing systems being introduced.	T
Information Security	
• The Hospice will establish and maintain policies for the effective and secure management of its information assets and resources.	A
• The Hospice will promote effective data confidentiality and information security practices to its staff through policies, procedures and training.	N, R, S, E
• The Hospice will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of data confidentiality and information security.	F, P

	Appendix 1
Information Quality Assurance	
• The Hospice will establish and maintain policies and procedures for information quality assurance and effective management of data records.	B, U
• Directors, Senior Managers and Managers are expected to take ownership of, and seek to improve, the quality of information within their services.	A
• Data quality standards will be set through clear and consistent definition of data items, in accordance with national standards.	
• The Hospice will promote information quality and effective records management through policies, procedures/user manuals and training.	A, B

4. Related Policies and Procedures

A range of related policies and procedures fall under Information Governance as it combines both Clinical Governance and Corporate Governance. Procedures have been put in place to support the confidential handling of information within the Hospice and the sharing of this information with other organisations. A schedule of such policies and procedures is set out in Appendix 1. Correlation of those with various elements of the 4 key strands of the IG Policy are indicated in Section 3 above.

5. Responsibility and Accountability

The Board of Trustees is responsible for ensuring that sufficient resources are made available to support the implementation of IG policy and procedures in order to ensure compliance with legal and professional requirements.

The Chief Executive is the designated IG Lead in the Hospice and is overall responsible for overseeing the health and application of IG within the Hospice; developing and maintaining policies, standards, procedures and guidance, coordinating IG in the hospice, raising awareness of IG and ensuring there is ongoing compliance with the policy and its supporting standards and guidelines.

The Director of Patient Services is the designated IG Clinical Lead in the Hospice (and is also the named Caldicott Guardian – refer Section 5 herein) and is responsible for application of IG policy and procedures in the clinical domains, and for completing the Data Security and Protection Toolkit assessment.

The Senior Management Team members are required to take ownership of the IG policy and related policies and procedures within their respective departments and services, and to ensure adequate understanding and awareness of IG among their staff.

All Staff whether permanent, temporary or contracted, employees and volunteers alike, are responsible for ensuring that they remain aware of the requirements incumbent upon them for achieving compliance on a day-to-day basis. These include maintaining confidentiality of data, ensuring secure storage of data and being aware of situations where disclosure may be required or may not be required.

6. Caldicott Guardian

The Director of Patient Services is the Caldicott Guardian incorporating the following responsibilities within the Clinical domain:

- Acting as champion for data confidentiality at operational levels.
- Developing knowledge of confidentiality and data protection matters including links with external sources of advice and guidance.
- Ensuring that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- Overseeing all arrangements, protocols and procedures where confidential healthcare information may be shared with external bodies including disclosures to other public sector agencies and other outside interests.

7. Monitoring this Policy

This policy will be reviewed annually by the Chief Executive and Senior Management Team, resulting in recommendations for any necessary enhancements, or a statement of no changes required, to be submitted to the Board of Trustees for their review and approval.

8. Sanctions

Non-adherence to the IG policy and related policies and procedures will be investigated by either the relevant Line Manager or such other designated individual as appointed by the Chief Executive. Breach of this policy could lead to disciplinary action. Depending on the circumstances this could range from remedial training to dismissal, always in accordance with applicable employment legislation and Hospice HR guidelines.

Appendix 1

Policies

A. IS1 - Information Security Procedures and Guidelines

B. G7a - Policy and Procedure for Health Records: Creation, Management, Storage & Destruction

C. G7c - Policy on Information for Patients

D. G7d - Access to Health Records

E. G7b - Confidentiality of Health Records

F. CP11 - Procedure for Reporting Significant Events or Accident Incident Report (A.I.R) Form

G. G4 - Management Risk Policy

H. G4b - Disaster Management Procedure

I. G6 - Media Policy

Procedures

M. **Staff Confidentiality Code of Conduct** (Policy G7b sets out the standards expected of staff in maintaining the confidentiality of patient information);

N. **Staff Access Control and Password management** (IS1 sets out procedures for the management of access to computer-based information systems);

O. **Data Transfer** (IS1, G7 and G7d sets out procedures around the secure transfer of data, collecting consent and maintaining confidentiality within the hospice);

P. **Incident management** (CP11 or Accident Incident Report (A.I.R) form sets out the procedures for reporting a security breach, however you should respond by letting your manager or senior manager know asap);

Q. **Business Continuity** (G4 Management Risk Policy and G4b Disaster Management Procedure sets out the procedures in the event of system failure);

R. **Portable Device Staff Guidelines** (IS1 and G7 provides guidance for staff use on the use of portable devices);

S. **IG Training** will be included in induction for all staff. Online training for clinical staff and general training including reading relevant policies for all others. Evidence held with training department;

T. G7i – Procedure for Disposal of Confidential Waste;

U. G7g – Procedure for Data Protection by Design and Data Privacy Impact Assessments (DPIA).