Lindsey Lodge Hospice & Healthcare

INFORMATION GOVERNANCE POLICY

Contents

1 Introduction

1.1 Background

The purpose of this document is to inform Lindsey Lodge staff on Information Governance Policy.

Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health and social care service and Fundraising Environment. It provides a consistent way for employees to deal with the many different information handling requirements including:

- Information governance management
- Clinical information assurance for safe service user care
- Supporter/Donor Information
- Confidentiality and data protection assurance
- Corporate information assurance
- Information security assurance
- Secondary use assurance

1.2 Aims

The aims of this document are:

- To maximise the value of organisational assets by ensuring that data is:
    - Held securely and confidentially.
    - Obtained fairly and lawfully.
    - Recorded accurately and reliably.
    - Used effectively and ethically.
    - Shared and disclosed appropriately and lawfully.

- To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental. Lindsey Lodge will ensure:
    - Patient/Personnel Information will be protected against unauthorised access.
    - Patient/Personnel Information will be shared appropriately.
    - Confidentiality of information will be assured.
    - Integrity of information will be maintained.
    - Information will be supported by the highest quality data.
    - Regulatory and legislative requirements will be met.
    - Business continuity plans will be produced, maintained and tested.
    - Information security training will be available to all staff.
    - All breaches of information security, actual or suspected, will be reported to, and investigated by the Data Protection Officer or Caldicott Guardian
    - Supporter/Donor information will be used appropriately

2 Scope

This policy applies to all staff working for or on behalf of Lindsey Lodge, including permanent staff, bank staff, volunteers and any placement students.

3 Roles and Responsibilities

3.1 Chief Executive

Overall accountability for Information Governance across the organisation lies with the Chief Executive who has overall responsibility for establishing and maintaining an effective Information Governance culture within the organisation, for meeting all statutory requirements and adhering to guidance issued in respect of Information Governance.

3.2 Caldicott Guardian

The Medical Director has been appointed Caldicott Guardian. They will:

- Ensure that Lindsey Lodge satisfies the highest practical standards for handling patient or service user identifiable information.
- Facilitate and enable appropriate information sharing and make decisions on behalf of Lindsey Lodge following advice on options for lawful and ethical processing of information, in particular in relation to disclosures.
- Represent and champion Information Governance requirements.
- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- Oversee all arrangements, protocols and procedures where confidential patient or service user information may be shared with external bodies.

3.3 Senior Information Risk Officer (SIRO)

The Chief Executive has been nominated as Senior Information Risk Owner. They will:

- Take overall ownership of the organisation's Information Risks that sit within the Risk Register (L Drive/Risk and Governance/Risk Register).
- Act as champion for information risk on the IT & IG Committee and provide written advice to the Chief Executive on the content of the organisation's statement of internal control in regard to information risk.
- Understand how the strategic business goals of Lindsey Lodge maybe impacted by information risks, and how those risks may be managed.
- Implement and lead the Information Governance Risk Assessment and Management processes within Lindsey Lodge
- Advise the IT & IG Committee on the effectiveness of information risk management across the Organisation.
- Receive training as necessary to ensure they remain effective in their role as SIRO.

3.4 Data Protection Officer/Information Governance Lead

The Business Manager as Data Protection Officer will:

- First point of contact on all data protection matters
- Responsible for overseeing data protection strategy and implementation to ensure compliance with Data Protection.
- Maintain an awareness of information governance issues within Lindsey Lodge.
- Review and update the information governance policy in line with local and national requirements.
- Ensure annual assessments using the Data Security & Protection Toolkit are carried out.
- Review and audit all procedures relating to this policy where appropriate on an ad-hoc basis.

3.5 IT & IG Committee

The IT & IG Committee has a terms of reference and a delegated authority to act from the Board of Trustees, reporting via the Finance & Business Development subcommittee to the board.
They have organisational responsibilities for the following areas in relation to Information Governance:

- Support organisational compliance of Data Security & Protection Toolkit requirements
- advising and contributing to the overall quality of the service;
- ensure that an appropriate comprehensive information governance framework and systems are in place throughout the organisation and in line with national standards
- ensure that information governance and information security training is made available and taken up by staff as necessary to support their role.
- ensure the organisation's approach to information handling is communicated to all staff and made available to the public.
- ensuring compliance with all applicable legal and regulatory requirements, in particular those of CQC and Information Commissioners Office.
- ensuring that internal audit is consistent with the governance needs of the organisation.
- ensuring that risk management and internal control is appropriate and of the highest standard, escalating risks to the Finance Committee via the organisation's risk register.
- offer support, advice and guidance concerning Information Governance/Security and Data Protection issues.
- Provide a focal point for the resolution and/or discussion of Information Governance issues
- ratifying relevant policies and guidelines.
- reporting after each meeting to the Finance Committee any issues of concern or action using highlight reporting.

3.6 Line Managers

Line managers will take responsibility for ensuring that staff are adequately trained and that the Information Governance Policy is implemented within their team.

3.7 All Staff

It is the responsibility of each employee to adhere to the policy. Staff will receive instruction and direction regarding the policy from a number of sources:

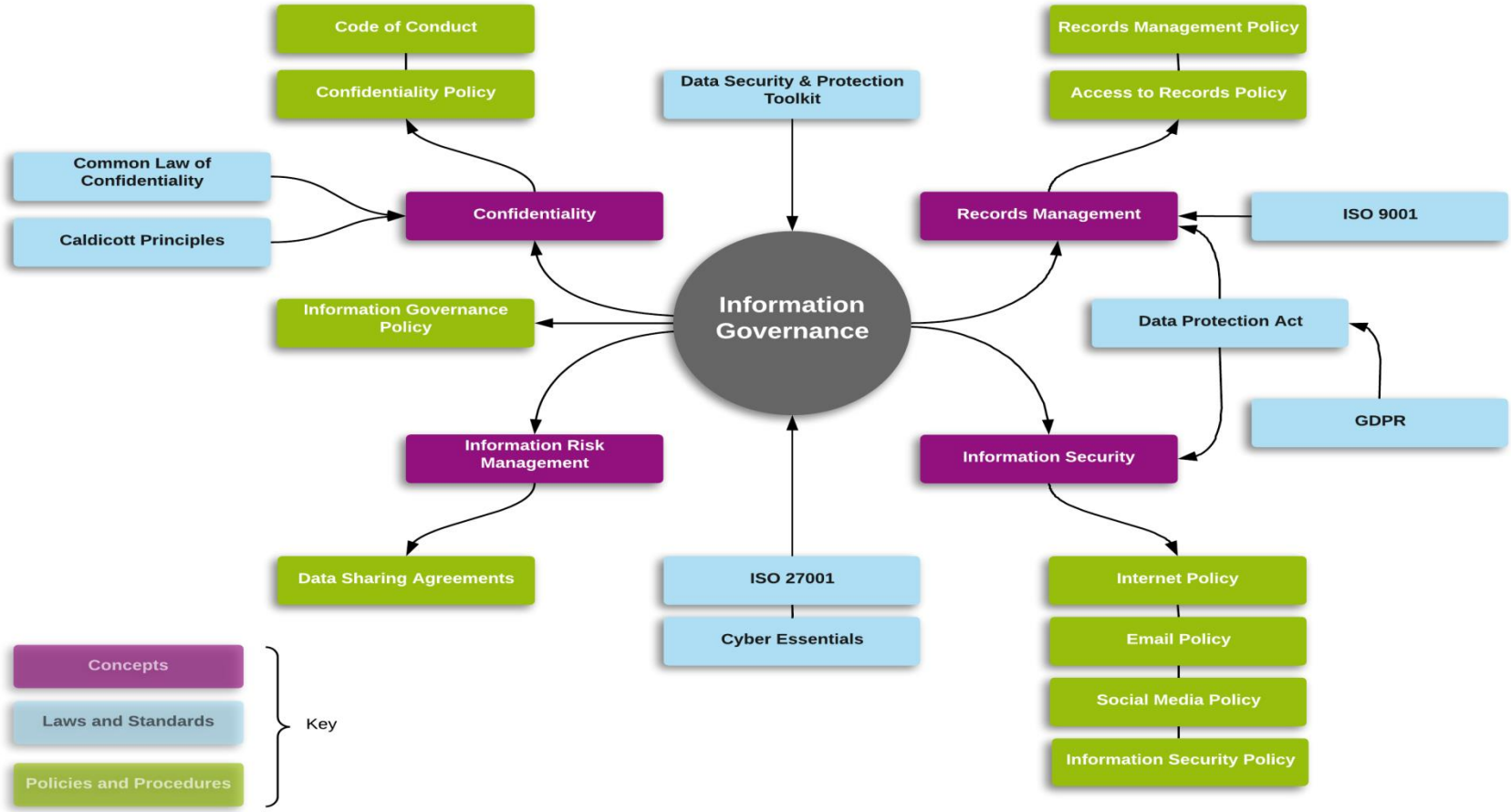
- Line manage.
- Specific training course.
- Clinical and Non Clinical mandatory training
- Other communication methods, for example, team meetings.

4 Information Governance Policy Framework

Lindsey Lodge has developed a framework for its Information Governance Policy. This is supported by a set of Information Governance policies and related procedures to cover all aspects of Information Governance which are aligned with the NHS Operating Framework and the Information Governance toolkit requirements and in our Partnership agreement for IT Security with F4 IT.

4.1 Overview

Information Governance is comprised of a number of policies, procedures, standards and best practice. The following diagram illustrates how all the key elements interact.



4.2 Policies

The key Information Governance Policies at Lindsey Lodge are:

Policies	
Information Security Policy	This policy is to protect all information assets to a consistently high standard. The policy defines security measures applied through technology and encompasses the expected behaviour of those who manage information within the organisation.
Records Management Policy	This policy is to promote the effective management and use of information, recognising its value and importance as a resource for the delivery of corporate and service objectives. It also provides guidance on how to deal with a Subject Access Request for access to relevant confidential records including Health & Safety and Supporter/Donor records
Confidentiality and Data Protection Policy	This policy lays down the principles that must be observed by all who work within Lindsey Lodge and have access to personal or confidential business information. All staff must be aware of their responsibilities for safeguarding confidentiality and preserving information security in order to comply with common law obligations of confidentiality, the NHS Confidentiality Code of Practice and the Data Protection Act.
Email Use Policy	The purpose of this policy is to ensure the appropriate and effective use of e-mail within Lindsey Lodge. It sets out the rules governing the sending, receiving and storing of e-mail; establishes user rights and responsibilities for the use of the system; and promotes adherence to current legal requirements and standards.
Data Security Breach Management Policy	This policy details the process staff should adhere to in the event of a data security breach and who to contact. There are 4 key elements to breach management which includes: Containment and recovery, assessment of ongoing risk, notification of breach and evaluation and response and ensures staff are aware of their personal responsibilities in the event of a data security breach.
Social Media Policy	This policy provides guidance on how Lindsey Lodge staff can use social media professionally, ethically and lawfully without compromising patient or donor or staff confidentiality
Internet Use Policy	This policy determines how Lindsey Lodge staff can use the Internet professionally, ethically and lawfully without compromising service user or staff confidentiality, whilst maintaining the security of the IT network.

A contractual clause requires that all staff must read and adhere to all information security policies.

4.3 Procedures and Guidance

A number of other procedures and guidance are used to assist the IG Framework including:

- Registration Authority Procedures
- The NHS Confidentiality Code of Practice
- NHS Care Records Guarantee
- Records Management: NHS Code of Practice
- Caldicott Guidance
- Data Security & Protection Toolkit

4.4 Legislation

Lindsey Lodge shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act
- General Data Protection Regulation
- The Data Protection (Processing of Sensitive Personal Data) Order
- The Copyright, Designs and Patents Act
- The Computer Misuse Act
- The Health and Safety at Work Act
- Human Rights Act
- Regulation of Investigatory Powers Act
- Health & Social Care Act
- The Public Records Act
- The Common Law Duty of Confidentiality
- Mental Capacity Act

4.5 Data Security and Protection Toolkit

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

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.

Annual plans will be developed year on year from the DSPT to ensure all requirements are met

4.6 Key Governance Bodies

The following forums/committees regularly meet to deliberate on information governance issues -

- IT & IG Committee
- Board of Trustees

4.7 Risk Management

The ability to apply good risk management principles to IG is fundamental and Lindsey Lodge e will apply them through organisational policies. Risk assessments will be completed by the relevant individuals within Lindsey Lodge with support from the SIRO and the Data Protection Officer where required for any IG risk related issue.

4.8 Training and Guidance

All staff will attend an Induction which incorporates IG Training. Where staff and volunteers have access to patient/supporter/donor information they must complete on line e-learning annually, through E-Lfh, provided by NHS England. When this is not appropriate they must read the "Information Governance Mandatory Training Booklet" and sign to say this has been read and understood. This will be recorded on staff care.

In subsequent years all staff as part of mandatory clinical and non-clinical training will have Data Security & IG refresher training in accordance with the organisation's mandatory training policy.

4.9 Incident Management

All IG incidents will be reported through the Lindsey Lodge Incident management system, on the Incidents & Accidents database held on our L drive. This must be reported to the Caldicott Guardian, IG Lead, SIRO, Data Protection Officer or Chief Executive straight away. The process of addressing the incident will be managed to ensure compliance with IG principles, in line with the Data Security Breach Management Policy. Significant issues will be subject to full investigation and reporting action and may need reporting to the ICO within 72 hours.

Where the incident is a result of a breach of policy by a member of staff, this could result in disciplinary proceedings.

4.10 Investigation

The Caldicott Guardian with support from the SIRO and Data Protection Officer will be responsible for the investigation of all IG issues reported. This may include but is not limited to, breaches of policy, breaches of confidentiality and issues related to IT Security.

4.11 Awareness and Advice

The IT & IG Committee will provide advice on any IG related issue. They will support the production of newsletters and all staff e-mails to provide up to date information to staff on IG issues.

All staff are made aware of new and reviewed policies via the monthly team Talk briefing, team meetings and manager meetings. All policies are made available via the L drive.

5 Consultation

IT & IG committee

6 Dissemination

Via Lindsey Lodge `L` drive policies/guidelines of this form.

7 Equality Act

In accordance with the Equality Act (2010), Lindsey Lodge will make reasonable adjustments in the workplace so that an employee with a disability, as covered under the Act, should not be at any substantial disadvantage. We will endeavour to develop an environment within which individuals feel able to disclose any disability or concern which may have a long term ad substantial effect on their ability to carry out their normal day to day activities.

Lindsey Lodge will wherever practical make adjustments as deemed reasonable in light of an employee's specific circumstances and the Hospice's available resources paying particular attention to the Disability Discrimination requirements and the Equality Act (2010)

REFERENCES: Care Plus Group (LLH IT provider), ICO website, Data Protection Act 2018				
Lead Author of Policy: Kay Fowler, IT Support Officer **Responsible Sub-group IT & IG Committee** **RATIFICATION DATE BY TRUSTEES 26th February 2019 (5th July, 2018)** Review interval 3 years				
TO BE REVIEWED	REVIEW COMPLETED	BY	APPROVED BY	CIRCULATION
February 2021	July 2021	KF	IT/IG Committee	L: Policies & Guidelines
July 2024				