FedBucks

Information Governance Policy

Policy Number:	FBIG01
Last Review Date:	July 2018
Approving Body:	FedBucks Board
Date of Approval:	October 2018
Implementation Date:	May 2018
Next Review Date:	January 2019
Review Responsibility:	Director for Governance
Target Audience:	All Staff
Version:	2

Approval and Authorisation

Completion of the following detail signifies the review and approval of this document, as minuted in the senior management group meeting shown.

Version	Authorising Group	Name of Approver	date
1.0	Fedbucks Board	Karen Gill	Jul 2018
2.0	FedBucks Board	Karen Gill	Oct 2018

Change History

Version	Status	Reason for change	date	Author
2.0	Await approv	Change in front sheet	21/05/18	K Lovegrove
2.0	Approved	Inclusion of data protection officer role	03/10/18	K GIll

Document References

Ref #	Document title	Document Reference/Location

1. Introduction

1.1. The role of FedBucks is to deliver healthcare. This policy will help all staff and contractors to understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

1.2. The purpose of this document is to provide guidance to all FedBucks staff and contractors involved in the delivery of its services.

1.3. 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 service. 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 Patient Care.
- Confidentiality and Data Protection assurance.
- Corporate Information assurance.
- Information Security assurance. and
- Secondary use assurance.

1.4. The aims of this document is:

- 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, and
    - Shared and disclosed appropriately and lawfully.

- To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental. FedBucks will ensure:

    - Information will be protected against unauthorised access.
    - 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, and
    - All breaches of information security, actual or suspected, will be reported to, and investigated by the Head of Corporate Information Governance.

2. Scope

2.1 Staff within the Scope of this Document

Staff working in or on behalf of FedBucks (this includes contractors, temporary staff, secondees and all permanent employees).

3. Roles and Responsibilities

3.1 Chief Executive

3.1.1 Overall accountability for procedural documents across the organisation lies with the Chief Executive. As the Accountable Officer that has overall responsibility for establishing and maintaining an effective document management system and the governance of information, meeting all statutory requirements and adhering to guidance issued in respect of information governance and procedural documents.

3.2 Caldicott Guardian

A member of the FedBucks Board has been appointed the Caldicott Guardian. Who will:

- Ensure that FedBucks satisfies the highest practical standards for handling patient identifiable information.

- Facilitate and enable appropriate information sharing and make decisions on behalf of FedBucks following advice on options for lawful and ethical processing of information, in particular in relation to disclosures.

- Represent and champion Information Governance requirements and issues at Board level.

- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff, and

- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, Fedbucks.

3.3 Senior Information Risk Owner (SIRO)

A member of the FedBucks Board has been assigned the role of SIRO who will:

- Take overall ownership of the organisation's Information Risk Policy.

- Act as champion for information risk on the Board

- Understand how the strategic business goals of FedBucks may be impacted by information risks, and how those risks may be managed.

- Advise the Board on the effectiveness of information risk management across the FedBucks

- Receive training as necessary to ensure they remain effective in their role as SIRO.

3.4 Information Asset Owners

3.4.1 Information Asset Owners (IAO) will:

- Lead and foster a culture that values, protects and uses information for the benefit of patients.

- Know what information comprises or is associated with the asset, and understands the nature and justification of information flows to and from the asset.

- Know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy.

- Understand and address risks to the asset, and providing assurance to the SIRO.

- Ensure there is a legal basis for processing and for any disclosures, and

- Refer queries about any of the above to the Head of Corporate Information Governance.

3.5 Director of Governance

3.5.1 The Director of Governance will:

- Maintain an awareness of information governance issues within FedBucks.

- Review and update the information governance policy in line with local and national requirements.

- Review and audit all procedures relating to this policy where appropriate and

- Ensure that line managers are aware of the requirements of the policy.

3.6 Systems Manager

3.6.1 The Systems Manager will ensure:

- The formulation and implementation of ICT related policies and the creation of supporting procedures, and ensuring these are embedded within the service developing, implementing and managing robust ICT security arrangements in line with best industry practice;

- Effective management and security of the FedBucks ICT resources, for example, infrastructure and equipment;

- Developing and implementing a robust IT Disaster Recovery Plan;

- Ensuring that ICT security levels required for Data Security and Protection Toolkit are met;

- Ensuring the maintenance of all firewalls and secure access servers are in place at all times, and;

- Act as the Information Asset Owner for the ICT infrastructure with specific accountability for computer and telephone equipment and services that are operated by corporate and clinical work force, e.g. personal computers, laptops, personal digital assistants and related computing devices, held as a NHS asset.

- Undertake the Data Protection Officer role and responsibilities

3.7 Line Managers

3.7.1 Line managers will take responsibility for ensuring that the Information Governance Policy is implemented within their staff and contractors
.

3.8 All staff

3.8.1 It is the responsibility of each employee to adhere to the policy.

3.8.2 Staff will receive instruction and direction regarding the policy from a number of sources:

- Policy/strategy and procedure manuals;
- Line manager;
- Specific training course;
- Other communication methods, for example, team meetings; and
- Staff Intranet.

3.8.3 All staff are mandated to undertake the Bluestream 'Information Governance' during their induction period.

3.8.4 Information governance training is required to be undertaken on an annual basis.

3.8.5 All staff must make sure that they use the organisation's IT systems appropriately, and adhere to the Acceptable use of ICT Policies.

4. Information Governance Policy Framework

4.1 FedBucks is developing 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 its Corporate and BHT's Operating Framework (24/7 service) and the Data Security and Protection toolkit requirements.

4.2 The Key Information Governance Policies will be added to the policy in 6 months' time on completion of the Data Security and Protection Toolkit.

5 **Training Plan**

5.1 A training needs analysis will be undertaken with Staff affected by this document.

5.2 Based on the findings of that analysis appropriate training will be provided to Staff as necessary.

6. Monitoring

8.1 Compliance with the policies and procedures laid down in this document will be monitored via the Admin & Governance Manager in Bucks 24/7 and the Deputy Operations Manager in Planned Care and the Planned Care Operations Director for the Corporate Functions.

8.3 The Director of Governance is responsible for the monitoring, revision and updating of this document on an annual basis or sooner if the need arises.

7 Data Processing Impact Assessments

7.1 All new services will require a Data Processing Impact Assessment to be carried out. This will involve the Services Operations/Governance Manager, FedBucks Systems Manager and Director of Governance.