FedBucks
Data Protection Policy

Policy Number:	FBIG03
Last Review Date:	
Approving Body:	FedBucks Board
Date of Approval:	October 2018
Implementation Date:	July 2018
Next Review Date:	July 2021
Review Responsibility:	System Manager
Target Audience:	All Staff
Version:	1.0

CONTROLLED DOCUMENT

This document is uncontrolled once printed.

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	Dominic Wood	Oct 2018

Change History

Version	Status	Reason for change	date	Author

Document References

Ref #	Document title	Document Reference/Location

Introduction

The Data Protection Act 2018 (DPA) requires a clear direction on policy for security of information held within FedBucks and provides individuals with a right of access to a copy of information held about them.

FedBucks needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include patients, employees (present, past and prospective), suppliers and other business contacts. The information we hold will include personal, sensitive and corporate information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018.

The lawful and proper treatment of personal information by FedBucks is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. We ensure that FedBucks treats personal information lawfully and correctly.

This policy provides direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information.

See also: Subject Access Request Policy, which covers accessing information held by Fedbucks under the Data Protection Act.

1.0 Data Protection Principles

We support fully and comply with the six principles of the Act which are summarised below:

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained/processed for specific lawful purposes, and will only be used for the purpose for which it was collected.

3. Personal data held must be adequate, relevant and not excessive.

4. Personal data must be accurate and kept up to date, and every reasonable step will be taken to ensure any personal data that is inaccurate is erased or rectified without delay.

5. Personal data shall not be kept for longer than necessary.

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data.

2.0 Employee Responsibilities

All employees will, through appropriate training and responsible management:

- comply at all times with the above Data Protection Act principles
- observe all forms of guidance, codes of practice and procedures about the collection and use of personal information
- understand fully the purposes for which FedBucks uses personal information
- collect and process appropriate information, and only in accordance with the purposes for which it is to be used by FedBucks to meet its service needs or legal requirements
- ensure the information is correctly input into FedBucks's systems
- ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required
- on receipt of a request from an individual for information held about them by or on behalf of immediately notify FedBucks manager
- not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian / IG Lead
- understand that breaches of this Policy may result in disciplinary action, including dismissal

3.0 Practice Responsibilities

FedBucks will:

- Ensure that there is always one person with overall responsibility for data protection. Currently this person is the System Manager should you have any questions about data protection. The Governance Director will take on these responsibilities if the first named individual is absent with illness or on annual leave.
- Maintain its registration with the Information Commissioner's Office
- Ensure that all subject access requests are dealt with as per our Access to Medical Records policy
- Provide training for all staff members who handle personal information
- Provide clear lines of report and supervision for compliance with data protection and also have a system for breach reporting

- Carry out regular checks to monitor and assess new processing of personal data and to ensure FedBucks's notification to the Information Commissioner is updated to take account of any changes in processing of personal data

- Develop and maintain DPA procedures to include: roles and responsibilities, notification, subject access, training and compliance testing

- Display a poster in the waiting room explaining to patients FedBucks' policy (see below).

- Make available a leaflet on Access to Patient Information, for the information of patients. Also display the certificate of registration with the Information Commissioners office.

- Take steps to ensure that individual patient information is not deliberately or accidentally released or (by default) made available or accessible to a third party without the patient's consent, unless otherwise legally compliant. This will include training on confidentiality issues, DPA principles, working security procedures, and the application of best practice in the workplace.

- Undertake prudence in the use of, and testing of, arrangements for the backup and recovery of data in the event of an adverse event.

- Maintain a system of "Significant Event Reporting" through a no-blame culture to capture and address incidents which threaten compliance.

- Include DPA issues as part of FedBucks general procedures for the management of risk.

- Ensure confidentiality clauses are included in all contracts of employment.

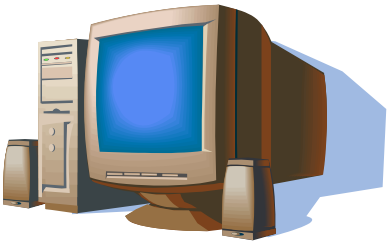
- Ensure that all aspects of confidentiality and information security are promoted to all staff.

- Remain committed to the security of patient and staff records.

- Ensure that any personal staff data requested by the CCG or NHS, i.e. age, sexual orientation and religion etc., is not released without the written consent of the staff member

PATIENT POSTER

DATA PROTECTION ACT – PATIENT INFORMATION



We need to hold personal information about you on our computer system and in paper records to help us to look after your health needs, and FedBucks' clinicians and staff are responsible for their accuracy and safe-keeping. Please help to keep your record up to date by informing us of any changes to your circumstances.

Doctors and staff at FedBucks have access to your medical records to enable them to do their jobs. From time to time information may be shared with others involved in your care if it is necessary. Anyone with access to your record is properly trained in confidentiality issues and is governed by both a legal and contractual duty to keep your details private.

All information about you is held securely and appropriate safeguards are in place to prevent accidental loss.

In some circumstances we may be required by law to release your details to statutory or other official bodies, for example if a court order is presented, or in the case of public health issues. In other circumstances you may be required to give written consent before information is released – such as for medical reports for insurance, solicitors etc.

To ensure your privacy, we will not disclose information over the telephone or fax unless we are sure that we are talking to you. Information will not be disclosed to family, friends, or spouses unless we have prior written consent, and we do not leave messages with others.

FedBucks Limited complies with GDPR in all our dealings with your personal data. Medical information will be kept confidential and will only be disclosed to those involved with your treatment or care, including your GP, and, if applicable, to any other person or organisation who may be responsible for your treatment or for funding your care. Under the GDPR regulations effective from 25 May 2018, we will only keep your information as long as is necessary and in accordance with the retention periods set out in the Department of Health's Record Management Code of Practice for Health and Social Care 2016. All records are destroyed confidentially once their retention period has been met and we have made the decision that the records are no longer required.

You have a right to see your records if you wish. Please ask a FedBucks HCA if you would like further details and our patient information leaflet.