FedBucks

Computer Usage Policy

Policy Number:	FBIG11
Last Review Date:	February 2019
Approving Body:	FedBucks Board
Date of Approval:	October 2018
Implementation Date:	September 2018
Next Review Date:	Feb 2022
Review Responsibility:	System Manager
Target Audience:	All Staff
Version:	2.0

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	Martin Thornton	Jul 2018
2.0	QA Committee	Liz Hooker	Feb 2019

Change History

Version	Status	Reason for change	date	Author
2.0		Removal of named individuals in key roles and replaced with role titles and reference to Board Assurance Framework contact list	01/02/2019	Lynda Moorcroft

Document References

Ref #	Document title	Document Reference/Location

Contents

1. Background

FedBucks recognises the considerable potential for the use of information and communications technology and will work positively to facilitate appropriate development and innovation. Computer facilities are provided to support staff in fulfilling the responsibilities of their roles.

It is an essential legal prerequisite of connection to the NHS network that any NHS organisation establishes and operates an effective policy for the use of computers. This is designed to protect the wider community of NHS organisations from unauthorised and inappropriate use whilst ensuring the security and confidentiality of identifiable or sensitive data.

This policy has been developed from relevant legislation including the Data Protection Act 2018 and the Computer Misuse Act, and from NHS guidance contained primarily in the Caldicott requirements and from "Ensuring Security and Confidentiality in NHS Organisations" – the NHS IM&T Security Manual. They are therefore requirements that the FedBucks is obliged to follow.

2. Purpose and objectives

This policy document sets out a Code of Conduct that applies to all staff who use computer facilities provided by the FedBucks and/or who are required to carry out remote working either at home or other remote location.

It explains the behaviour and obligations expected of staff when using any of the FedBucks computer systems.

Key roles referred to in this Code are identified in Appendix A.
Key objectives of the policy:

- Confidentiality – data access is confined to the reasons listed below to ensure the confidentiality and protection of business or person sensitive information retained by the FedBucks.
    - a specific authority to view
    - a need to know
    - a need to use

- Integrity – all system assets are operating correctly according to specification and in the way the current user believes them to be operating. Access should be restricted to authorised users only.

- Availability – information is delivered to the appropriate individual where and when it is required.

3. Secure Use of FedBucks Information – key statements

It is essential that staff comply with FedBucks policy in relation to secure information handling. Please refer to the FedBucks Confidentiality Code of Practice - Appendix 1 Information Handling Responsibilities (see ref [5]) for more detailed information.

3.1 For the continued confidentiality of patient and staff data it is generally expected that no patient or staff identifiable data will be taken for use outside FedBucks locations or legitimate places of work.

3.2 For most purposes, fully anonymising or pseudoanonymising the data will allow it to be used without compromising confidentiality, for research for example.

3.3 It is recognised however, that in exceptional circumstances there may be a need for legitimate removal. In these cases the individual must understand the risks involved and must make the decision whether or not to remove sensitive data or to take the safer and more secure form of anonymised or pseudoanonymised option. Management approval must be sought prior to the removal of data.

3.4 Personally owned IT equipment must not be used for the processing or storage of person identifiable, confidential or sensitive data.

3.5 All donated or loaned IT Equipment to the FedBucks e.g. personal computers, laptops or other mobile devices such as tablets and smartphones must be risk assessed, approved, registered and encrypted with the System Manager **prior** to any use – excluding BHT 24/7 equipment our Partner Organisation.

3.6 ALL portable IT media e.g. laptops, DVD's, CD's, USB devices/memory sticks or keys containing person identifiable data, regardless of its use must be secured using approved industry standard AES 256 encryption software. Exceptions can only be made by the Senior Information Risk Owner (SIRO).

3.7 No FedBucks computing hardware or software may be removed from FedBucks premises, other than for the purpose of transportation between FedBucks sites or other places of work, without prior written permission from the line manager.

4. Inappropriate Use of Computers

FedBucks resources or facilities must never be used to assist or support any illegal activity. For example, to create, edit, access or disseminate pornographic, sexist, racist material or any other material likely to cause offence to staff, patients and visiting members of the public, via e-mail, Internet or any other method.

Under the provisions of the Computer Misuse Act, unauthorised access to computers (hacking) is illegal and must never be undertaken.

Storage of personally owned files such as music and photographs, e.g. wedding and holidays, on FedBucks file servers is forbidden. Any such files will be deleted without notice.

Personal USB sticks must **NOT** be used to data copy to, only to read from.

If sensitive data (PID) must be transferred then a FedBucks-authorised encrypted memory stick must be used. Please contact the System Manager for further information.

FedBucks computers and other IT equipment are provided to support the FedBucks's legitimate business requirements.

Perrsonal/private use is not acceptable.

5. Danger from Viruses and Malware

Computer viruses and malware can be extremely harmful to computer systems and all reasonable precautions to prevent their spread must be taken. e.g. never open an email attachment from an unknown source; do not load data from any external storage device without first running virus checking software. For further guidance read the FedBucks Virus Control Procedure.

6. Access to Computer Systems

Requests for access to the FedBucks computer systems will be provided during Induction of Staff as appropriate. If you require access to previously unavailable systems contact the Systems Manager.

7. Systems Access

7.1 Access to corporate systems will only be given once adequate training has been received and competence levels have been reached as determined by the trainer/systems manager, for example Adastra and Rotamaster.

7.2 Where systems are not under the control of System Manager (locally implemented and maintained) training must be administered by the local management.

8. Password Disclosure

8.1 Staff will ensure that all personal passwords used remain strictly personal to that member of staff and are not disclosed in any form.

8.2 They must not be relayed verbally, written down or otherwise revealed to any other individual either within or outside the FedBucks.

8.3 If any person accesses information through the use of another person's password then both individuals may be subject to action in accordance with the FedBucks' disciplinary policy.

8.4 The wilful or negligent disclosure of confidential information whether written or digital could be seen as gross misconduct under the FedBucks' Disciplinary policy and may lead to dismissal.

8.5 In some instances it may be necessary for IT to know a users' password in order to fix a problem with a PC. At such times IT will arrange with the user to change the password on completion of the task.

8.6 Some systems require the use of a smartcard to log in. Staff who need to use a smartcard for this purpose must ensure that it is kept secure at all times when not in use and not loaned or otherwise used by any other person. Failure to do so may result in disciplinary action.

8.7 Staff using a smartcard must ensure that it is removed from the card reader once their session is complete.

9. Password / PIN Management

9.1 Any system capable of using passwords/ PIN's must have the facility enabled.

9.2 Length of password/ PIN numbers and characteristics are system dependent and are therefore defined by reference to the appropriate System Manager.

9.3 Passwords must include a combination of alpha, capital and numeric characters, in any order.

9.4 Passwords/ PIN numbers must be unique to the system i.e. not be used for access to other systems.

9.5 Passwords/ PIN numbers must not be shared with or disclosed to anyone.

9.6 Frequency of password / PIN number change is system dependent and passwords MUST be changed at the frequency defined in a table in Appendix 1 appropriate to the system. The default is 60 days (30 days for system administrators).

9.7 Passwords/ PIN numbers must be changed if security is believed to have been, or actually has been, breached.

9.8 Administrative and system passwords must be changed when an administrator or system manager leaves the organisation.

9.9 Passwords must not be a combination of characters that is likely to be guessed such as a family name, nickname, DOB, car registration or consecutive characters e.g. ABC123.

9.10 Passwords/ PIN numbers must be something memorable so that it doesn't need to be written down. Passwords are encrypted (coded) when applied, and therefore cannot be seen by the system administrators

10. Logging into Computer Systems

Staff may have use of a variety of methods to login to a computer system, for example this may be your user name or swipe card. All of these methods are for personal access only and must not be used to provide third party access. Care must be taken to ensure that login methods are kept secure at all times. Loss of swipe cards must be reported immediately to the System Manager and reported as an incident using FedBucks' Adverse Incident and Significant Event Form in accordance with the FedBucks Adverse Incident and Significant Event Policy.

Staff have an individual responsibility to ensure that they log themselves out of systems after use or if leaving a system unattended for any period. Only authorised staff may view data and it is essential that staff understand that no one else, except themselves, should have the opportunity to add, amend, view or delete data under their personal log in access rights

11. Removal of System Access

System Administrators and Managers are empowered to remove or suspend access to systems in the event of a security issue or other breach of this policy.

System access will be removed under the terms of the User Account and Email Usage Policy.

12. Portable Media

All portable media devices for use on devices owned or operated by the FedBucks are covered by this policy. This includes but is not limited to:

- Smart devices, e.g. smart phones,
- USB Memory Sticks,
- tapes
- external hard drives
- external optical drives for DVD's and CD-Roms
- Laptops. The FedBucks has a separate Mobile Device Security Policy.

All portable media capable of storing information must be encrypted prior to use. The System Manager will be able to provide advice on this.

Any personal mobile phone which has the capability to access NHS Mail and download documents and files which may contain person identifiable and sensitive information falls under the category of portable media. Since they are not supplied or approved by the FedBucks and will not be encrypted by the IT Services department they **must not** be used in this way under any circumstances.

Any procurement for portable media must be made through the System Manager.

Data stored on portable media must not serve as the primary source of data. The FedBucks' network drives must be the original source of data to act as a backup in the event of loss or theft.

Portable media must only be used for the purpose of transporting data and not for the long term storage of data. Once the media has arrived at its destination and the data copied to its new location the portable media must be securely wiped or securely destroyed. Please contact the System Manager for further information.

FedBucks staff or contractors are not permitted to introduce or use any portable media other than those provided and explicitly approved by FedBucks. The System Manager can provide information on the FedBucks-approved memory stick.

Portable media supplied by FedBucks is either owned or managed by the System Manager and must be appropriately security marked to indicate this.

Under no circumstances should person identifiable or sensitive information be downloaded on to portable media that is not encrypted.

All portable media must be securely transported and protected against loss, damage and misuse and locked away when not in use.

Tampering with portable media in order to bypass encryption security is not permitted.

13. Access to Person Identifiable Information

Person identifiable information should only be accessed on a "need to know" basis and only by authorised individuals.
It is a breach of FedBucks' policy and may result in disciplinary action or constitute a criminal offence if a member of staff accesses:

- their own personal staff or health records

- the records of colleagues, family, friends or others

Where there is no legitimate business need such access is deemed inappropriate and is therefore not an authorised FedBucks requirement.

To disclose or share confidential information where there is no legitimate business relationship, specific business need or is not on required on a “need to know basis” (e.g. selling of information for personal gain, general indiscretion or “gossip”) constitutes gross misconduct and will lead to disciplinary action, possibly leading to criminal charges.

14. IT Remote Working

Explicit authorisation from both the appropriate System Manager and the Department Head of Operations must be obtained prior to being granted access to remote working and will **only** be authorised once appropriate risk assessments have been satisfied. Personally owned IT equipment must not be used for the processing or storage of person identifiable, confidential or sensitive data e.g. home working, off site.

Please refer to Appendix B – Guidance using IT Remote Working to access Person Identifiable, Confidential or Sensitive Data, the associated request form is available using the icon shown in Section 6 which is available on your PC Desktop.

15. Software Licenses

All software must be used in accordance with the licenses agreed when purchased and described in the copyright statement in those licenses. Further copying of software is illegal and copying of software should never be undertaken without express permission from the System Manager.

Modified versions of licensed software must only be incorporated in programs written by users with the express written permission of the licensor.

Reverse engineering or de-compiling of licensed software must only be undertaken with the express written permission of the licensor.

All copies of software loaned must be removed and returned from any computer owned by an employee at the end of the period of employment, or when requested to do so.

16. Installing Software and Creating Systems

Software must not be installed on any FedBucks computer system which forms part of, or can be connected to, any FedBucks departmental, specialty or corporate computer system without the prior written permission of the System Manager.

Communications equipment must not be installed on any FedBucks computing resource without prior written approval from the FedBucks System Manager.

The creation, installation or introduction of any computer based information software system for the purpose of storing or processing sensitive data requires notification and prior approval from the FedBucks’ Caldicott Guardian, the System Manager or SIRO.

17. Loss or Theft of FedBucks IT Equipment

Any loss or potential loss including theft or damage of FedBucks' IT equipment must be reported immediately to the System Manager, to the member of staff's line manager and via the FedBucks' Adverse Incident and Significant Event Form in accordance with the FedBucks' Adverse Incident and Significant Event Policy. Theft of IT equipment must also be reported to the FedBucks SIRO and the police to obtain a crime number.

18. Monitoring and Auditing Access to Confidential Information

FedBucks' Board have an overall responsibility for monitoring and auditing access to confidential personal information. Day to day responsibility rests with the System Manager and Department Mangers.

The following are examples of events that the FedBucks may audit:

- failed attempts to access confidential information;
- repeated attempts to access confidential information;
- successful access of confidential information by unauthorised persons;
- evidence of shared login sessions/passwords;

Investigation and management of confidentiality events will be in line with the FedBucks' Adverse Incident and Significant Event Policy. Depending on the severity and circumstances of the incident, staff may be subject to disciplinary procedures resulting in suspension, supervised access to systems, re -training, termination of employment/ contract or criminal charges.

19. Breach of Policy

All incidents or information indicating a suspected or actual breach of this policy must be reported as soon as possible to the immediate line manager and where appropriate the System Manager. Staff may be subject to disciplinary procedures if this policy is not adhered to.

20. Monitoring the Policy

The System Manager will monitor the implementation of this procedure and subsequent revisions through:

- Ensuring that all staff requiring access to IT systems or a requirement to work electronically on FedBucks business remotely have access to and understand the requirements of the Policy.
- Regular review of reported information security incidents

21. Review of This Document

This document will be formally reviewed every 3 years.

This document will be subject to revision when any of the following occur:

- The adoption of the standards highlights errors and omissions in its content
- Where other standards / guidance issued by FedBucks conflict with the information contained herein
- Where good practice evolves to the extent that revision would bring about improvement

22. Glossary/Definitions
The following terms/acronyms are used within the document.

- System - any computer or other electronic device where software accesses or otherwise carries out functions on information held electronically – for example Personal Computer, Server, PDA.
- PDA - Personal Digital Assistant, e.g. Palm Pilot, Blackberry.
- PIN Personal Identification Number
- Malware Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system. This software is usually installed covertly by means of an email attachment, for example, by tricking the user into an unwanted action.
- PID Person Identifiable Data

Appendix A Key Roles

Caldicott Guardian – Nominated Director

SIRO – Service Development Director

DPO - Systems Manager

Information Governance – Planned Care Director, Nominated Director

Appendix B

Data Protection Considerations when Remote Working

All staff should adhere to FedBucks policy when using FedBucks records/information for remote working purposes. In addition, consideration should be given to the following:

Manual records (paper records)

- Staff should avoid taking patient records home whenever possible, and where this cannot be avoided, procedures for safeguarding the information should be made i.e. locked securely in a briefcase, kept under your supervision at all times or locked in a secure cupboard with only your access, until they are returned to work
- Confidential/Sensitive information should not be left where it might be looked at by unauthorised persons i.e. family and friends and should not be left in insecure areas
- Records must not be left in the car. During transportation these should be locked in the boot of the car and removed immediately on arrival at home and kept secure as above.
- Records must be properly booked out from their normal filing system i.e. tracing and tracking system
- Records must be returned to the filing location, as soon as possible

Electronic records

- Always log-out of any computer system or application when you have finished working or leaving your work station for a period of time
- Ensure passwords are kept safely and not accessible to friends and family
- Use a password protected screen saver to prevent casual viewing of information
- Do not store patient information on a USB stick unless you have been authorised to do so and it is a FedBucks standard encrypted USB stick. The data must be wiped from the memory stick once it has been copied to its destination.
- Do not download person identifiable/sensitive information from your NHS mail account onto your home PC or any other non-FedBucks provided equipment

Key Risks to working on personally owned equipment

- You cannot guarantee adherence to the FedBucks' Security Policies by members of your family or friends
- You would be unable to guarantee virus protection to the FedBucks' standard
- Even if you delete any FedBucks' data from your home PC, this is still retrievable from the hard drive by an expert or with the right software
- IT equipment is vulnerable to theft and loss and any data stored on personally owned equipment that does not meet the FedBucks' strict security requirements are at a significantly higher risk.