Birmingham and Solihull NHS
Mental Health NHS Foundation Trust

INFORMATION SYSTEMS SECURITY POLICY (ISSP)

Policy Number & Category	**IG 02**	**Information Governance**
Version Number & Date	**Version 3.7**	**February 2009**
Ratifying Committee	**Clinical Governance Committee**	
Date Approved	**March 2009**	
Next Review Date	**March 2011**	
Executive Lead	**Executive Director of Finance & Resources, Chris Tidman**	
Policy Lead	**Deputy Director of IM&T – IT Services, Paul Lewis**	
Policy Author	**Head of IT Operations, Alan Dodsworth**	
Formulated Via The	**Information Quality Assurance and Information Governance Strategy Group**	

Policy Statement

The Information Systems Security Policy (ISSP) has been developed to protect the Trust and its employees from hazards and threats, to ensure business continuity and to minimise any business damage by preventing and reducing the impact of information systems security incidents.

The policy enables information to be shared, but ensures the secure protection of that information and related IM&T assets.

Birmingham and Solihull NHS
Mental Health NHS Foundation Trust

Key information systems security policy components

The IS Security Policy has three basic components (confidentiality, integrity and availability), intended to preserve adequate security of information systems:

- **Confidentiality**: protecting sensitive information from unauthorised disclosure.
- I**ntegrity**: safeguarding the accuracy and completeness of information and computer software.
- **Availability**: ensuring that all vital services, information and/or data systems are available to users when required.

Table of Contents

1 Introduction

This document defines the Information Systems Security Policy (ISSP) for Birmingham and Solihull Mental Health NHS Foundation Trust, hereafter known as BSMHFT. It forms a key component of BSMHFT overall information governance management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

The ISSP applies to all Trust business and covers the information, information systems, networks, and physical environments where information is processed or stored.

2 Objectives, Aim and Scope

2.1 Objectives

The objectives of this ISSP are to ensure the effective operation of information systems and that those systems are delivered when and where they are needed. It will preserve:

2.2 Confidentiality

- Access to data shall be confined to those with appropriate authority.

2.3 Integrity

- Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.

2.4 Availability

- Information shall be available and delivered to the right person, at the time when it is needed.

2.5 Policy aim

2.5.1 The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by BSMHFT by:

- Ensuring that all members of staff are aware of and comply with the relevant legislation as described in this and other associated policies.

- Describing the principles of security and explaining how they shall be implemented in the Trust.
- Introducing a consistent approach to security, ensuring that all members of staff understand their own responsibilities.
- Creating and maintaining within the Trust, a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the Trust.

2.6 Scope

2.6.1 This policy applies to all information, information media, information systems, networks, applications, locations in use by BSMHFT and organisations hosted by BSMHFT or supplied under contract to it.

3 Responsibilities for Information Security

3.1.1 All staff have a responsibility to ensure information security and to comply with all information security policies and procedures – failure to do so may result in disciplinary action.

3.1.2 Ultimate responsibility for information security rests with the Chief Executive of BSMHFT, but on a day-to-day basis, the Deputy Director of IM&T – IT Services (DDIT) shall be responsible for managing and implementing the policy and related procedures.

3.2 The responsibility for the security of an information system lies with the "owner" of that system. Owners of information systems may delegate their security to an individual or group but remain ultimately accountable for that system. DDIT will advise and monitor ownership. A detailed list of information systems and owners will be kept by the IM&T Department and monitored by the DDIT. An example of this file can be found in the following location:

http://intranet/ISSPDocs/Trust_Information_Assets.pdf

3.3 Line Managers are responsible for ensuring that their permanent and temporary staff and contractors and volunteers are aware of:-

- The information security policies applicable in their work areas.
- Their personal responsibilities for information security.
- How to access advice on information security matters.

3.4 All staff shall ensure that data confidentiality and integrity is maintained.

3.5 The ISSP shall be maintained, reviewed and updated by the DDIT, and shall be reviewed every two years unless a significant change is required.

3.6 Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

3.7 Each member of staff shall be responsible for the operational security of the information systems they use in their working environment. For example systems must be closed if work has been completed, or if leaving the desk for a short time, PCs must be either logged off or locked before leaving.

3.8 Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use are maintained to the highest standard.

3.9 When systems from third parties are to be implemented, underpinning contracts will be introduced to ensure that the staff or sub-contractors of the third party shall comply with all appropriate security policies. All requests such as this must use the Trust's IT Request for Change (RFC) process and be ratified by the Change Advisory Body*.

* The Change Advisory Body (CAB) consists of representatives from the IT Management team. Its function is to ensure all changes to IT services are managed to minimise the impact of the change and to assess its business need. The CAB has final sanction on whether a request for change can progress.

3.9.1 For further information on the Trust's RFC process follow this link:

http://intranet/IM_&_T/ITServices/RFC/RFC.htm

4 Legislation and NHS mandatory requirements

4.1 BSMHFT is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of BSMHFT who may be held personally accountable for any breaches of information security for

which they may be held responsible. BSMHFT shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001
- Access to Health Records Act 1991

4.2 In addition, the Trust will abide by the Department of Health (DoH) as well as the NHS Connecting for Health (CfH) Codes of Practice and Statement of Compliance.

5 Policy Framework

5.1 Management of Security

- At Trust Board level, responsibility for information security shall reside with the Executive Director responsible for IM&T.
- The DDIT (identified as the as the Information Security Officer within the Information Governance Toolkit) shall be responsible for implementing, monitoring, documenting and communicating security requirements for the Trust.

5.2 Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary. This will be in the form of updates on the Trust Intranet, Team Brief, Team Talk and global emails.
- An example of the Awareness Training Log can be found here:

http://intranet/ISSPDocs/Ongoing_training_log.pdf

5.3 Contracts of Employment

- Staff information security responsibilities shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

5.4 Security Control of Assets

Each key IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset. For example the corporate patient system (ePEX) custodian is the Deputy Director Clinical Systems (DDCS) and the Trust's email system custodian is the DDIT.

5.5 Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or electronic data storage hardware. Each area will have a secure access key pad or lock. When access to the area is required an entry will be recorded in the Access Control Log found in each area.

5.6 Computer Access Control

Access to computer systems shall be restricted to authorised users who have a business need to use the facilities. Access to computer systems are controlled initially by the Trust's Network Access Form with rights to specific systems ratified by the employee's line manager.

On completion of the Network Access Form the employee will be issued with a Network User ID and initial password. This will enable them to access corporate systems (email, Intranet etc).

Staff who leave the employment of the Trust will have their access to Information Systems revoked via the IT domain account deletion process.

5.7 Password Management

System account names and passwords are the principal means of validating access to information systems. It is the responsibility of all employees/users of BSMHFT information systems to maintain password integrity. **Under no circumstances should passwords to the Trust network or information systems be divulged, shared with anyone or left in a public place.**

5.8 Use of Information Systems

All users of information systems are responsible for ensuring their use is appropriate and care is taken to maintain and protect the integrity and quality of the data held on that system.

Staff should ensure that where service users are present in an area where systems are used, they do not come into contact with any login IDs or passwords and do not, under any circumstances use Trust PCs other than those recognised as Internet for Service User equipment.

5.9 Application Access Control

5.9.1 Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

5.9.2 Access to information systems are controlled initially by the Trust's Network Access Form with rights to specific systems ratified by the employee's line manager. Access to further systems should be processed through the Trust's IT Request for Change (RFC) process.

5.10 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. For example, information systems are housed with secure rooms locked with a key or secure number keypads. These areas are protected by fire and intruder alarms. Access to these areas is restricted to authorised personnel only. Desktop equipment is protected by secure access to the areas in which they are held and in more vulnerable areas by security cages. Authorised staff who enter these areas must complete an access control log detailing time of entry, exit and the nature of the work being carried out. These logs are regularly audited and reviewed by I.T senior staff.

Staff who use IT equipment used outside of Trust business premises for approved business activities shall take appropriate precautions to avoid damage or theft of equipment.

5.11 Equipment Disposal

IT equipment disposal is subject to NHS Guidelines for the disposal of IT Equipment and the Waste Electrical and Electronic Equipment (WEEE) legislation. BSMHFT has an approved process for the disposal of IT equipment to ensure that data is securely destroyed and confidentiality is maintained.

The guidelines for the disposal of IT equipment can be found here:

http://intranet/ISSPDocs/IT21_Disposal_of_PC_Guidelines.pdf

5.12 Information Risk Assessment

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within an IM&T risk register which forms part of the overall Trust Risk Register. The IM&T risk register is reviewed quarterly with the Director of IM&T and reported to the Risk Management Committee. Action plans and all associated actions shall be reviewed when appropriate. Any implemented information security arrangements shall also be a regularly reviewed feature of BSMHFT risk management annual programme, via the Risk Management Committee.

These reviews shall help identify lessons learnt and best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

The reporting of information security incidents is included on incident training and as part of the information governance induction, which is mandatory for all staff.

5.13 Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be reported to the Head of IT Operations (HITO). The HITO will then action and escalate to the DDIT. The incident will then be logged on the Information Incident Log which is regularly reviewed by the correlating Information Governance Sub Committee and where the Trust Incident System. All information security events shall be investigated to establish their cause and impact with a view to avoiding similar events.

5.14 Data Protection

BSMHFT has a designated Confidentiality Policy (*IG01 - Confidentiality Policy*) which incorporates the Data Protection Act 1984/98.

5.15 Data Storage

No work related or private data (in particular sensitive data) should be stored locally on PCs or laptops. Data should be stored on a Trust file server. Should access not be available, data can be stored on an Trust Standard Encrypted USB stick or locally if the PC or laptop has an encrypted disk drive.

Contact the Service Desk on 0121 301 5111 for further information.

5.16 Protection from Malicious Software (Computer Viruses)

BSMHFT shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on BSMHFT PCs or laptops without permission from the HITO or the DDIT. Data files generated or updated outside of the Trust on external media such as CDs, DVDs etc are potentially dangerous therefore they should not be used without first contacting the IT Service Desk to ensure they are safe.

Should a virus be detected on any PC, any use should cease and the incident must be reported ***immediately*** to the IT Service Desk on ext 0121 301 5111. The I.T Department will log and action the incident and advise when the PC can be used.

Further advice regarding Trust Standard secure USB sticks can be found on the IT Services page on the Trust Intranet or via the IT Service Desk.

5.17 Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis by system owners.

The Trust has in place routines to regularly audit compliance with this and other policies. In addition it reserves the ri ght to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts.
- Investigating or detecting unauthorised use of the system.

- Preventing or detecting crime.
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training).
- In the interests of national security.
- Ascertaining compliance with regulatory or self-regulatory practices or procedures.
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above Act and the Human Rights Act 1998 and will be subject to authorisation by the DDIT.

5.18 Accreditation of Information Systems

BSMHFT shall ensure that all new information systems, applications and networks include a security plan and are approved by the Trust's CAB as part of the formal RFC process before they commence operation. This security plan provides an overview of the security requirements of the system including the steps taken to protect the data housed and the responsibilities of the relevant systems stakeholders, e.g. information owners, users etc.

5.19 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Trust's CAB as part of the Trust's RFC process. There are however exceptions to this, for example changes to the Trust's main patient system (ePEX) is controlled by the DDCS.

5.20 Software Licensing

BSMHFT shall ensure that all information products are properly licensed and approved by the HITO or DDIT. Users shall not install software or applications on BSMHFT IT equipment. Should a requirement arise the request should follow the Trust's RFC process and be ratified by the CAB.

5.21 Data Encryption and the Use of Mobile or Portable Devices

The NHS Chief Executive has clearly stated that no personal identifiable information or other sensitive data should be stored or transported unencrypted on any portable media. In a further statement it was stated that 'any data stored on a PC or other removable device in a non-secure area or on a portable device such

as a laptop, PDA or mobile phone should also be encrypted to NHS standards.'

Therefore all laptops purchased by the Trust since Jan 2008 have been fitted with an encrypted hard drive as standard. Laptops purchased before then are not encrypted and should not be used to store any personal identifiable data. The Trust has introduced a standard secure USB memory stick for use on Trust PCs and laptops. This device is available via the IT Operations Team. These sticks are issued with guidance but essentially they will allow staff to transfer (not store) sensitive information between Trust sites and store non-sensitive information.

No USB Memory Sticks other than the BSMHFT standard secure memory stick can be used in BSMHFT IT Equipment.

The use of cameras, camera phones or other similar recording equipment is prohibited within the Trust without the permission of senior management. This applies particularly to clinical areas or where Service Users may be in attendance.

5.22 Procurement of IT Equipment/Devices

The procurement of all IT equipment is controlled by the IT team to ensure that the equipment required is appropriate to the need of the business and that it is compatible with existing systems and infrastructure. Staff wishing to purchase IT equipment must first complete an "IT Purchase Request Form". The requirement will then be assessed and authorised before being passed onto the Supplies Department for progression. A link to this document can be found below

http://intranet/IM_&_T/ITServices/Purchasing/Purchase_Request_Form.htm

6 Electronic Mail (Email) Use

6.1 Electronic mail (email) is the primary digital method of communicating within BSMHFT and is also widely used to communicate externally.

6.2 All employees of BSMHFT should ensure that information communicated via email is accurate and care is taken to ensure that the email cannot be misconstrued. As well as the Data Protection

Act's considerations, email communication is considered another form of publishing and therefore libel laws also apply.

6.3 The Trust issues guidelines for the use of the corporate email system within the Trust's Network Access Form, which can be viewed here.

http://intranet/IM_&_T/ITServices/NetworkAccess.htm

Employees may be held liable for any deviation from the email usage guidelines.

6.4 As email is the primary digital method of communicating both internally externally to the Trust all staff need to be mindful of the sensitivity of the data they are transferring (particularly patient identifiable information) via email and that data is secure. Below is a table detailing the various email routes that can be used in the Trust and whether they are secure.

xxx.xxx@bsmhft.nhs.uk	⟷	xxx.xxx@bsmhft.nhs.uk	**Secure**
xxx.xxx@nhs.net	⟷	xxx.xxx@nhs.net	**Secure**
xxx.xxx@bsmhft.nhs.uk	⟷	xxx.xxx@nhs.net	**Insecure**
xxx.xxx@bsmhft.nhs.uk	⟷	xxx.xxx@hotmail.com	**Insecure**
xxx.xxx@nhs.net	⟷	xxx.xxx@hotmail.com	**Insecure**

Note: In this table hotmail.com is an example of a web based email system. All other web based email systems such as those provided by popular search engines and Internet service providers (Yahoo mail, Google mail) are also insecure and should not be used for the transfer of sensitive data. If unsure contact the IT Service Desk on 5111.

There are a number of secure governmental email systems where personal identifiable information can be transferred providing it is sent via the NHS.Net email system not the BSMHFT system. Those systems are detailed in the following table:

National Heath Service network	*.nhs.net
Criminal Justice Secure email service	*.cjsm.net
Public sector organisations connected to the GSI community within the GSi	*.gsi.gov.uk

Public sector organisations connected to the GSX community within the GSi	*.gsx.gov.uk
Private sector organisations connected to the GSi who meet the required security standards	*.gse.gov.uk
Predecessor of the GSE used by private sector organisations	*.gssiup.co.uk
Police National Network or Criminal Justice Exchange	*.pnn.gov.uk *.pnn.police.uk
Private sector organisations connected to the Police National Network	*.scn.gov.uk

6.5 Email Inbox Storage and Limits

All staff have a finite amount of storage space on the Trust's email system. It is the responsibility of all staff to carry out regular housekeeping (deleting emails no longer required or archiving emails over a certain age) to enable them to continue to use the system. All managers are responsible for ensuring this happens.

Further advice can be obtained from the IT Service Desk on Ext (301) 5111

7 BSMHFT Corporate Electronic Mail (email) Disclaimer Statement

7.1 As a measure of good practice and to ensure compliance to the ISSP is being maintained and to mitigate any possible legal action being taken against BSMHFT employees, IM&T has adopted the following email disclaimer on all its email transmissions:-

This email may contain confidential information some or all of which may be legally privileged and subject to legislation; such as the Data Protection Act, the Freedom of Information Act, the Computer Misuse Act etc.

It is intended solely for the addressee. If you are not the intended recipient, please accept our apologies, do not read, use, copy, distribute, print or disclose any of the information contained within and inform the author immediately before deleting.

All views expressed in this email are those of the individual sender, except where the sender specifically states these to be the views of the BSMHFT.

7.2 Bulk Data Transfer

The Trust regularly has a requirement to transfer sensitive data to official organisations for example, patient data to commissioners for reporting purposes. This carried out using a Secure FTP (Fixed Transfer Protocol) system which is completely secure. All requests for this form of transfer are facilitated by the IT team. Please contact the Service Desk on 0121 301 5111 for further information.

7.3 BSMHFT Internet and Intranet facilities

The Internet/Intranet facility is provided by BSMHFT to help staff perform their work, so that they can access information, do specific work related research, learn about the application of new ideas/technologies and evaluate these effectively for potential benefits of the BSMHFT and its clients/staff alike.

The Internet service also exposes the Trust to potential threats (e.g. copyright violations; Infection by viruses, defamation, pornography and sexual harassment proceedings etc).

Guidelines on the use of the Internet is included in the Trust's Network Access Form which is completed and signed by all employees prior to access to the Trust's network, information systems, Internet and Intranet. Follow this link to view and Trusts Network Access Form:

http://Intranet/IM_&_T/ITServices/NetworkAccess.htm

Employees will be held personally liable for any deviation from this Intranet/Internet policy and it is in the employee's interest to adhere to this.

The Trust has introduced a service known as "Internet Access for Service Users". This allows service users to access the Internet under controlled conditions. Its use is regulated by a Local and Trustwide policy and any deviation from those policies will be reported to the appropriate manager and may result in the removal of the service to the relevant individuals or groups

7.4 Business Continuity and Disaster Recovery Plans

The Trust shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all clinical and business critical information, applications, systems and networks.

7.5 Revision

It is recommended that this policy be reviewed every two years or if a significant change is required.

8 Reporting, Audit and Further Information

8.1 Reporting

The Information Governance Steering Group (IGSG) shall keep the Trust Board informed of the information security status of the organisation by means of quarterly reports. The IGSG will be responsible for completing the IG Toolkit annually and reporting to the Trust Board.

8.2 Policy Audit

This policy shall be subject to audit by internal auditors commissioned by the Trust Board.

8.3 Further Information

Further information and advice on this policy can be obtained from the Deputy Director – IT Services, B1, 50 Summer Hill Road, Birmingham B1 3RB

8.4 Development, Consultation and Monitoring Process.

Consultation summary	
Date policy issued for consultation	18th December 2008
Number of versions produced for consultation	One
Committees / meetings where policy formally discussed	**Date(s)**
IG Strategy Group	5th February 2009
Clinical Governance Committee	3rd March 2009

Where received	Summary of feedback	Actions / Response

Draft Distribution and Comments:

IM&T Managers
IG Strategy Group
All Executive Directors
All Divisional Directors
All Programme Directors
All Clinical Directors

Glossary

Acronyms	Description
BSMHFT / 'The Trust'	Birmingham and Solihull Mental Health Foundation Trust
CAB	Change Advisory Body
CfH	NHS Connecting for Health

DDCS	Deputy Director Clinical Systems
DDIT	Deputy Director IM&T - IT Services
DoH	Department of Health
DPA	Data Protection Act
FTP	Fixed Transfer Protocol
HITO	Head of IT Operations
IG	Information Governance
IGSG	Information Governance Steering Group
IM&T	Information Management and Technology
ISSP	Information Systems Security Policy
NAF	Network Access Form
RFC	IT Request For Change
WEEE	Waste Electrical and Electronic Equipment

Link	Description
http://Intranet/ISSPDocs/IT21_Disposal_of_PC_Guidelines.pdf	Disposal of IT Equipment
http://intranet/IM_&_T/ITServices/NetworkAccess.htm	IT Network Access Form
http://intranet/IM_&_T/ITServices/Purchasing/Purchase_Request_Form.htm	IT Purchasing
http://intranet/IM_&_T/ITServices/RFC/RFC.htm	IT Request for Change
http://intranet/ISSPDocs/Ongoing_training_log.pdf	On going awareness Training
Risk Management Committee	Risk Management
http://intranet/ISSPDocs/Trust_Information_Assets.pdf	Information Assets