UNIVERSITY OF
OXFORD

NUFFIELD DEPARTMENT OF
PRIMARY CARE
HEALTH SCIENCES

Information Security Policy

Authorised by	Name: Richard Hobbs	Title : Head of Department
	Signature	Date: 23 February 2015

Commitment

The Nuffield Department of Primary Care Health Sciences (NDPCHS) has information and data in paper and electronic format. Many of our research studies involve collecting data from patients and participants in our research. We are grateful to all those patients and participants who take part and enable our studies, entrusting their data to us, and we commit to holding their data in the highest regard, protecting it as the law expects us to do.

We hold our employees and students (past, present and future) in high esteem and we commit to protecting information and data about them.

We expect members of the NDPCHS to protect, and hold confidential, information pertaining to the assets and operations of the Department and the University.

Introduction

Computer and information systems underpin all NDPCHS's activities, and are essential to

- Protect data, including patient, participant, employee and student data, in accordance with Data Protection Act;
- Ensure that information is only accessed by those authorised to do so;
- Ensure that the integrity of information is maintained so that it is accurate, up to date and available without disruption to the business of the Department;
- Protect other assets of the Department including intellectual property and financial information; and
- To safeguard the reputation of the Department and the University.

The NDPCHS recognises the need for its employees, students, tutors, honorary members and visitors to have secure access to the information they require in order to carry out their work, and recognises the role of information security in delivering this. Security of information must therefore be an integral part of the NDPCHS's management structure in order to maintain continuity of its business, legal compliance, and adherence to the University's own regulations and policies.

This information security policy defines the framework within which information security will be managed across the NDPCHS and demonstrates management direction and support for information security throughout the NDPCHS.

Scope

This policy is applicable to and will be communicated to all members of the Department which includes:

- employees of the department including casual staff;
- graduate students of Primary Care;
- graduate students of Evidence Based Health Care visiting or making use of NDPCHS offices and systems;
- honorary members, including honorary clinical tutors, of NDPCHS;
- visitors to NDPCHS; and
- contractors to NDPCHS.

It covers, but is not limited to, any systems or data attached to the NDPCHS's computer or telephone networks, any systems supplied by the NDPCHS, any data or information in paper format, any communications sent to or from the NDPCHS and any data – which is owned either by the University or the NDPCHS– held on systems external to the NDPCHS's network.

Organisation of Information Security

Professor Richard Hobbs, Head of Department is ultimately responsible for the maintenance of this policy and for compliance within the NDPCHS. This policy and subsidiary policies have been approved by the Senior Management Team.

Senior Management Team is responsible for reviewing this policy on an annual basis or when significant changes occur. It will provide clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.

The Senior Management Team is responsible for assessing identified security requirements and risks, approving risk mitigation strategies and controls, and accepting any residual risk

Nathan Hill is the Information Security Coordinator. He is responsible for the coordination of information security within NDPCHS and, specifically, will act as a point of contact for providing advice and guidance on the implementation of this policy.

Nicola Small, Departmental Administrator, is the Information Guardian, the departmental equivalent of a Caldicott Guardian. She is responsible for protecting the confidentiality of patient and participant information and enabling appropriate and lawful information sharing.

It is the responsibility of all line managers or supervisors to implement this policy within their area of responsibility and to ensure that all members of the Department for which they are responsible are 1) made fully aware of the policy; and 2) given appropriate support and resources to comply.

It is the responsibility of each member of the Department to adhere to this policy.

Policy Statement

The NDPCHS is committed to protecting the security of its information assets against loss or theft, breaches of confidentiality, failures of integrity or interruptions to availability.

The NDPCHS will adhere to the University's Information Security policy and support 'best practices' in the information security toolkit provided by IT Services.

All members of the department must undertake information security education, training and awareness appropriate to their responsibilities.

The minimum level of training for all members of the department is the Information Security Awareness Module

Members of the department working on clinical trials and research studies must undertake Good Clinical Practice training online or face to face as appropriate to their study.

Further free training particularly suitable for those working with NHS data is available to members of the University on the Health and Social Care Information Centre (HSCIC) Information Governance Training Tool.

Specialist advice on information security shall be made available throughout the NDPCHS and advice can be sought via the University's Information Security Team and/or OxCERT.

Failure to comply with this policy that occurs as a result deliberate, malicious or negligent behaviour, may result in disciplinary action.

Data Protection

The NDPCHS Information Security Policy applies to all Departmental information regardless of its form or physical location whereas the University's Policy on Data Protection refers to **personal data** only, not business information. The important differences from information security are:

- Data protection (DP) is about the law: Data Protection Act 1998 (DPA)
- DPA applies to personal data (PD) only
- DPA covers everything we do with PD, not just keeping it secure: how we collect it, how much we collect, what we do with it, how long we keep it, whether we can share it, etc.

All members of the department must read the IT Services Data Protection Guidance .

For the purposes of the Data Protection Act 1998 the department is registered under the University of Oxford, registration number: Z575783X

Risk Assessment and Reporting

To determine the appropriate level of security controls that should be applied a process of risk assessment shall be carried out. This is the responsibility of the Departmental Administrator.

An Information Asset Register will be maintained to record the type and location of the Departments information assets and the control measures to ensure their security.

Risk assessment outputs will be reported to the Information Security Team.

Records of the number of security breaches and their type will be kept and reported to the Senior Management Team.

NDPCHS will follow the University's policy for the escalation and reporting of security incidents and detected security incidents will be reported to oxcert@it.ox.ac.uk.

IT Rules

All staff are required to be aware of the University of Oxford regulations and policies applying to the use of University ICT Facilities.

All staff are required to be aware of and comply with the Medical Sciences Division (MSD) IT Services User Security Policy.

All staff are directed to the JANET acceptable Use Policy which details how University members are expected to use the Joint Academic Network. http://www.ja.net/services/publications/policy/aup.html.

The Department Information Security Policy will be made available to all new staff and highlighted in their induction packs, new starters will be required to have an IT induction (as part of the personnel induction) before using the IT systems.

University Card

All members of the Department will be issued with a University of Oxford Card. This card will enable the holder to access the Departmental office, become an authorised user of the Department computer network and to use the University of Oxford Nexus email system. The rights and responsibilities of University of Oxford card holders are detailed at: http://www.admin.ox.ac.uk/card/.

Building Security

Physical access to buildings in NDPCHS is controlled by auditable Salto card access systems that read a data chip in the University Card.

The Office Manager is responsible for ensuring that University Cards are programmed to allow members of the Department access to buildings.

The buildings have security cameras covering access points and are monitored 24 hours per day by the University Security Services.

NDPCHS office space is secured at building entrance points and at the entrance to NDPCHS space. Doors must never be left propped open and unattended.

If a University Card is lost it must be reported IMMEDIATELY to the Office Manager or a member of Departmental Administration so that building access can be stopped.

Individual offices are lockable by key. The Office Manager retains spare keys in a locked key press.

The electrical risers and the network/telecoms switch rooms are kept locked.

All staff have a lockable pedestal and lockable filing or storage space.

All confidential data in paper format must be stored in a locked cabinet. Individual study protocols may contain specific storage requirements that relevant members of the Department must follow. Research teams should consider whether or not a Systems Level Security Policy is needed for their study data.

Temporary visitors to the Department (those visitors that do not hold a University card) should be escorted by members of the Department and remain the responsibility of the member of the Department hosting them throughout their visit.

Network Security

The computer network is part of the University of Oxford network. It is provided, managed and backed up by MSD IT Services. All network policies are contained within the MSD IT Security Policy. This policy applies to all Departmental computer users.

Access to the computer network, and to specific network drives, is authorised by the Departmental Administrator under procedures set out in the MSD IT Security Policy.

Only computers authorised by MSD IT Services will be able to gain access to the computer network. These computers will have anti-virus software installed and provided by MSD IT Services which updates on connection to the network.

Network access is password protected and the password policy is set out in the MSD IT Security Policy.

Users must lock their computers when away from their desks (Ctrl+Alt+Del – Lock this computer).

Network servers are not encrypted. Any encryption should be done at file level. However MSD IT Services do provide a High Compliance System which offers additional security and should be considered as part of a Systems Level Security Policy by researchers who process and manipulate patient data.

All data should be stored on the network and NOT on the local hard-drive of a PC or laptop.

Members of the Department can access files on the network remotely using the Virtual Private Network (VPN) and logging in on the MSD IT Services netstorage site.

Users working off line can apply for an iFolder account to enable automatic data synchronisation.

The central IT Services provide the network infrastructure and the connection to the outside world. It supplies the first line defence against viruses, spam and a firewall.

E-mail

Members of the Department have a Nexus email account run, and scanned, by IT Services. More information about e-mail including security and junk-mail filtering is available at http://help.it.ox.ac.uk/email/index .

Sending an e-mail is as secure as sending a postcard.

Personal data must not be sent by e-mail. E-mail is potentially insecure - there are risks of interception, of using the wrong address, and of inappropriate forwarding.

Members of the department should consider the following alternatives to email:
OxFile
SharePoint
WebLearn
Granting the other person temporary access to folders/files

If there is no alternative to email, data must be sent as an encrypted attachment, using 7-zip. Encryption is also available in Word, Excel and Adobe. Do not email the password to unlock that file. Find another way to contact the recipient.

Dropbox and cloud storage

Dropbox servers are based outside the EU and therefore **must not be used** for sharing files containing Personal Data. Nor should Dropbox be used for other confidential information sharing.

Members of the department should consider OxFile, Sharepoint, Weblearn or shared network drives as a more secure alternative.

Disposal of Confidential Documents

Any documents containing personal data must be disposed of by shredding. Similarly all documents that contain confidential information, such as financial information, or information that might be regarded as an asset to the department must be shredded.

The Department provides ‘Shred It’ confidential waste boxes in several locations around the Department. These are secure, locked consoles. They are emptied regularly by uniformed, security screened staff, and the contents cross-cut shred on-site in locked trucks. The company provide a Certificate of Destruction each time they empty the consoles.

Information Transport

Wherever possible data and information should remain in the department, either physically or on network servers.

Members of the department should ensure that any paperwork containing data or information is kept securely with them until it can be brought into the office – it must not be left unattended (in cars for example).

Personal data or confidential information being posted out of the department must be in an envelope marked 'Confidential' and signature obtained for safe receipt.

Sharing of research data is complex and will depend on a number of factors, not least of which, in NDPCHS, will be the funder requirements.

Advice and information about sharing research data is available at http://researchdata.ox.ac.uk/. A data sharing plan should be created and advice sought from the Departmental Administrator as to whether a Data Sharing Agreement or other formal agreement should be put in place.

Personal data in electronic format must be transported on encrypted mobile devices and encypted when transferred electronically.

Advice on how to send documents securely is available at http://help.it.ox.ac.uk/infosec/protectyourself/documents/index

Back-up and Archiving

Network servers/drives are backed up every 24 hours by MSD IT Services. Data should not be stored on individual hard-drives not least because is not backed up.

All data must be archived appropriately when it is no longer required within the Department in accordance with the study protocol.

Hardcopy data must be boxed, recorded and removed to offsite secure storage. The Department has a contract with Restore Document Management. Details of facilities for archiving are detailed in the Department Archival Procedure.

Identifiable data, if archived electronically must be encrypted. If possible identifiable data should not be archived.

Encryption

All departmental laptops and personal laptops used to hold University data MUST be encrypted using the Whole Disc Encyption (WDE) service provided by the University through the MST IT Services team.

Where there is a strong and valid reason why WDE is not appropriate then a risk assessment must be prepared and written permission must be obtained for each laptop without WDE from the Head of Department. Permission will only be granted in rare instances. Members of the department should be aware that even where personal data is not stored on the local hard-drive it may still be stored temporarily on local cached memory.

USB sticks and external hard drives should be used with caution and MUST NEVER contain unencrypted personal data (PD). In most cases the safer option is to purchase encrypted

USB sticks and external hard drives. The exception to this is video interviews with study participants where integrity and quality of the video may suffer – in this case the video files must be strongly password protected.

Members of the department taking data out of the UK should not have an expectation of data privacy as devices may be searched and users may be compelled to provide decryption keys for any encrypted data.

Members of the department should check, before travelling, whether or not their destination country permits encryption software or has specific regulations on its use.

Mobile devices

All devices used to access University e-mail or documents must have a complex password to prevent unauthorised access. The standard 4 digit pin is not sufficient and must be disabled in favour of a complex password.

The advice on mobile security available at http://www.it.ox.ac.uk/policies-and-guidelines/is-toolkit/mobile-security-smartphones-tablets must be followed.

Mobile phones must have encryption enabled where it is available.

The following checklist must be detached from this Policy document, completed by each member of the Department and returned to Karen Gardner who will retain a copy.

Information Security Checklist

Name	
Date of Completion	
Signature	

Compulsory

- □ I have read and understood the Information Security Policy
- □ I have read the University Regulations regulating the use of information technology facilities
- □ I have read the IT Services Data Protection Guidance and I understand what data needs to be protected
- □ I know how to report loss of data or security breaches
- □ I know how to report the loss of University cards/keys/fobs etc.
- □ I understand how to securely share and transport data (or where to find this information before I do so) and
- □ I will use encryption on all mobile devices used to store Personal Data
- □ I will not give my University card to anyone else to use
- □ I will lock my PC when I am away from my desk and lock away any papers containing confidential information or Personal Data
- □ I will use complex passwords to access University e-mail, networks and other systems
- □ I will use a complex password on all mobile devices used to access University e-mail or documents
- □ I will not share my passwords with anyone
- □ I will not re-use my University password(s) outside the University
- □ I have undertaken the Information Security Awareness Module

Role dependent

- □ My GCP training is up to date and at the appropriate level
- □ I have undertaken the HSCIC training Introduction to IG for General Practice
- □ I have undertaken the HSCIC training Information Security Guidelines