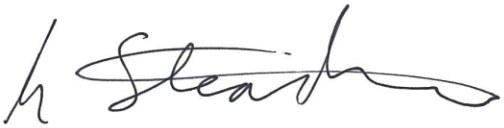
Nuffield Division of Clinical Laboratory Sciences Information Security Policy and Best Practice

Effective date: 15 July 2013

Author	Leon Steadman	Information Security Manager, IT Officer
		Date 16/10/15
Reviewed by	Sylvain Phaneuf	Systems Manager, Compliance (MSD IT)
		Date 16/10/2015
Reviewed by	Erin Gordon	Senior Administrator
		Date 16/10/15
Authorised by	Prof Alison Banham	Head of Division
		Date 16/10/15

Contents

1.1 Introduction

1.1.1 The policy is designed to ensure that the Nuffield Division of Clinical Laboratory Sciences ("NDCLS") will comply with all relevant compliance legislation in respect of information security. The policy will describe specific Nuffield Division of Clinical Laboratory Sciences rules and best practice on information security and reference any supervening policies of the University of Oxford ("the University"), the Medical Sciences Division ("MSD") and the Radcliffe Department of Medicine ("RDM") that will describe policy in more detail.

1.2 Policy Statement

1.2.1 The purpose and objective of this Information Security Policy is to protect the Nuffield Division of Clinical Laboratory Sciences information assets from all threats from a loss of confidentiality, integrity and availability, whether internal or external, deliberate or accidental.

1.3 Scope

1.3.1 This policy is intended for all staff and any visitors using the Nuffield Division of Clinical Laboratory Sciences IT systems, data or any other information asset.

1.3.2 For the purposes of this Policy the term "staff" will be taken to mean paid employees, authorised associate members, honorary members and academic visitors to Nuffield Division of Clinical Laboratory Sciences.

1.4 Roles and responsibilities

1.4.1 The Policy is authorised by the Head of Division of Nuffield Division of Clinical Laboratory Sciences.

1.4.2 The Nuffield Division of Clinical Laboratory Sciences Information Security Committee ("the Committee") is the Designated Owner of the Information Security Policy.

1.4.3 The Information Security Manager for the Nuffield Division of Clinical Laboratory Sciences is Leon Steadman.

1.4.4 The IT Officer for Nuffield Division of Clinical Laboratory Sciences is Leon Steadman.

1.4.5 The Data Controller for the Nuffield Division of Clinical Laboratory Sciences is the current University of Oxford Data Protection Officer: https://www1.admin.ox.ac.uk/councilsec/compliance/dataprotection/contacts/

1.4.6 The Council of the University has ultimate responsibility for information security within the University. More specifically, it is responsible for ensuring that the University complies with relevant external requirements, including legislation.

1.4.7 For the purposes of the Data Protection Act 1998, Nuffield Division of Clinical Laboratory Sciences is registered under the University of Oxford, registration number: Z575783X.

1.5 Information Security Policy Ownership and Responsibility

1.5.1 The roles and responsibilities of the designated Information Security Manager are to manage information security and to provide advice and guidance on implementation of the Information Security Policy.

1.5.2 The Designated Owner of the Information Security Policy has final responsibility for maintaining and reviewing the Information Security Policy.

1.5.3 It is the responsibility of all line managers to implement the Information Security Policy within their area of responsibility.

1.5.4 It is the responsibility of each member of staff to adhere to the Information Security Policy.

1.6 Nuffield Division of Clinical Laboratory Sciences Information Security Committee

1.6.1 The Committee shall consist of:

The Head of Division of the Nuffield Division of Clinical Laboratory Sciences
The Senior Administrator
The Information Security Manager
The IT Officer

1.6.2 Frequency of Committees

The Committee shall meet at least once a term.

1.6.3 The committee can co-opt staff to sit on the Committee as the need arises.

1.7 Audit and review

1.7.1 The Information Security Manager will be responsible for arranging and monitoring regular audits of all aspects of the Information Security Policy. The results of audits will be recorded and logged. Audits will be carried out no less than annually.

1.7.2 The Information Security Policy will be reviewed annually by the Information Security Manager and approved by the Information Security Committee.

1.8 Regulatory and Legislative Requirements

1.8.1 The Information Security Policy is designed to ensure that all regulatory and legislative requirements will be met.

1.9 Authentication and Authorisation

1.9.1 All members of staff will be issued with a University Card. This card will give authority for the member to become a user of the Medical Sciences Division IT Services ("MSD IT") computer network and to use the University of Oxford Single Sign On ("SSO") authentication system. The rights and responsibilities of University of Oxford card holders are detailed at http://www.admin.ox.ac.uk/card/

1.9.2 The MSD IT computer network is administered via a Novell system. Applications for a Novell username are processed by the MSD IT administrative team.

1.9.3 Passwords, SSO and Novell accounts must not be shared or disclosed to any third party.

1.9.4 Temporary visitors, e.g. contractors, will not be granted access to a computer account. Physical access to the buildings and offices will only be allowed during working hours or if accompanied by a member of staff.

1.9.5 Windows operating system users on desktop computers are required to use the Novell network login whenever possible in order for MSD IT to facilitate the management of the computers, i.e. automatic updating of anti-virus protection and installing the latest security patches. This does not apply to non-networked machines and users of other operating systems, e.g. Mac OS or Linux.

1.9.6 Remote access via the University's virtual private network ("VPN") client or *Eduroam* wireless network is authenticated with an additional Remote Access account obtained from the University's central IT Services: http://help.it.ox.ac.uk/network/remote/index/

1.10 Internet and email usage

1.10.1 Internet access is provided by the Joint Academic Network ("JANET") via the University's network, which is managed by IT Services. MSD IT network infrastructure connects Nuffield Division of Clinical Laboratory Sciences to the University's network.

1.10.2 All users of the network are required to be aware of the JANET Acceptable Use Policy which details how University members are expected to use the network. New staff will be informed of these rules as part of the induction process. These rules are also available at https://community.jisc.ac.uk/library/acceptable-use-policy

1.10.3 All users of the network are required to be aware of the University of Oxford Rules on Computer Use. New staff will be informed of these rules as part of the induction process. These rules are also available at http://www.it.ox.ac.uk/rules

1.10.4 All members of staff are expected to have read, understood and adhere to the MSD IT Security Policy available at http://www.imsu.ox.ac.uk/content/msd-it-services-security-policy. Every new starter will be informed of the MSD IT Security Policy (see 1.12.1) and have an IT induction before using the IT systems.

1.10.5 The use of email is controlled by IT Services and is covered by the University's Information, Communications Technology Committee ("ICTC") *Regulations 1 of 2002* (with subsequent amendments), available at http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml (Regulation 7 is particularly relevant to the transmission of electronic mail) and is overseen by the IT Officer.

1.10.6 Breaches of any policy rules will in the first instance be reported to the line manager and then a record of the breach should be passed to the IT Officer.

1.10.7 If users redirect or forward their emails to external mail servers they must ensure a comparable level of security as the University service.

1.10.8 Users are advised to beware of phishing exploits when using email. Always seek advice and in general be suspicious of emails with web links. See http://www.it.ox.ac.uk/infosec

1.10.9 Users are advised to familiarise themselves with the mail filtering facilities to minimise unwanted emails. See http://help.it.ox.ac.uk/email/filter/index

1.10.10 IT Services particularly encourages users to report phishing scams asking for passwords to University systems in order to protect other users and the University as a whole. See http://help.it.ox.ac.uk/email/phishing/index

1.11 Network and Systems IT Security

1.11.1 The Nuffield Division of Clinical Laboratory Sciences computer network is part of the University of Oxford network and is managed by system administrators of the MDS IT on behalf of the University Medical Sciences Division.

1.11.2 The MSD IT Service Specification can be viewed here: http://www.imsu.ox.ac.uk/content/msd-it-service-specification with particular attention to *Expectations and Responsibilities of Departments.*

1.11.3 Personally owned computers and devices will normally use either the IT Services wireless network in conjunction with a VPN client or an ethernet socket (if available) in order to connect to the network.

1.11.4 Connecting an unregistered computer to an ethernet socket will route to the Visitor Network which requires either a guest user account (obtainable from the IT Officer) or connecting to the University VPN in order to access the network. This method of connection may be preferable in areas of poor wireless reception or when a fast connection is required (wireless connections are restricted in speed).

1.11.5 It is not permitted to create *ad hoc* wireless networks, e.g. using devices such as Apple Airport Express or a wireless router.

1.11.6 Many incoming protocols including file sharing and printing are blocked at the NDCLS subnet (in our case 129.67.4.0/22) firewall. Web servers that are not registered (such as personal computers with web sharing turned on) cannot be accessed through the subnet firewall. Applications for web server registration should be made to IT Services.

1.11.7 Incoming access through the firewalls for such as licence servers and specified file services can be arranged at the discretion of MSD IT.

1.11.8 Users needing to use printers outside their subnet are required to use the MSD IT-managed Novell iPrint client or web interface: http://iprint.imsu.ox.ac.uk/ipp

1.12 Computers, Software and Hardware

1.12.1 Control measures for NDCLS hardware and software are defined in the MSD IT Security Policy: http://www.imsu.ox.ac.uk/content/msd-it-services-security-policy

1.12.2 The IT Officer is responsible for ensuring that the systems are risk assessed, audited and tested.

1.12.3 Line managers will ensure that their staff are adhering to the NDCLS Information Security Policy. Any breaches will be reported in the first instance to the IT Officer.

1.12.4 Any new software application should where practical be subject to validation and control before installation. Proper risk assessment should be employed on all projects that are developing new applications.

1.12.5 All software purchased will normally be required to comply with MSD IT Security Policy with respect to supported operating systems, appropriate authentication and resistance to abuse.

1.12.6 In general MSD IT-managed computers allow full administrator access rights to personal computers. Whilst this allows flexibility of working, such rights carry the responsibility of operating the computer in a sensible way.

1.12.7 Whilst users can install software on their personal computers this should not compromise the MSD IT pursuing its security policies. For example MSD IT provides anti-virus/malware software and system updates. It is not permitted to install further software for the purpose of disabling automatic system updates.

1.12.8 Essential non-compliant software, for example to control an instrument, must be installed on a non-networked computer. In particular Windows XP is no longer supported for security updates by Microsoft and so it is not permitted to connect a computer with this operating system to the network, unless special arrangements have been made to place such a computer on a restricted virtual local area network ("VLAN"). Such installations will be subject to additional controls to mitigate the risk of data loss and malware infection.

1.12.9 Your attention is drawn in particular to software which runs as a server, for example bioinformatics software which uses a database server.

1.12.10 Purchasers of software and hardware are advised to consult the IT Officer prior to making a purchase.

1.12.11 Personally owned and/or licenced software can be installed but must be removed when staff leave NDCLS. This includes Apple operating systems and upgrades.

1.13 Back-up and Archiving

1.13.1 Electronic data should be appropriately backed up using the University's Tivoli Storage Manager ("TSM") system and/or proprietary software e.g. Apple Time Machine. If using a proprietary system, backups should be located off-site wherever possible.

1.13.2 IT Services provide the data backup (using TSM) and long-term archive service both using the Hierarchical Filing System ("HFS") for the backup of University-related work. This service is available to University staff, senior members and postgraduates. Guidelines for acceptable use of HFS backup services can be found at http://help.it.ox.ac.uk/hfs/policy/acceptuse

1.13.3 MSD IT is responsible for the daily backup of all files stored on the MSD IT file servers.

1.13.4 It is the responsibility of individual staff members to ensure their data is appropriately backed up.

1.13.5 All data must be archived appropriately when they are no longer required.

1.13.6 Hardcopy data must be recorded and moved to secure storage. The security level of archive storage must be the subject of a risk assessment which takes into account the nature of the data to be stored.

1.14 Encryption

1.14.1 No data of a sensitive nature and no personally identifiable data will be removed from NDCLS under any circumstances unless appropriate measures are in place.

1.14.2 Staff wishing to take sensitive work away from Nuffield Division of Clinical Laboratory Sciences, for example taking confidential results to discuss with a collaborator or working at home, will be required to store their work on an encrypted USB memory storage device. Such devices are available for purchase from MSD IT: http://www.imsu.ox.ac.uk/content/encryption-services

1.14.3 Encryption will not be used on standard electronic storage unless a risk assessment highlights the need.

1.14.4 The University offers a Whole Disc Encryption ("WDE") service for University owned computers in the Medical Sciences Division. Contact the IT Officer to request WDE. N.B. System encryption is mandatory for University computers taken away from NDCLS (see 1.15.8).

1.15 Remote Access and Home Working

1.15.1 Any member of staff wishing to work from home must notify the Deputy Administrator Personnel and have understood the precautions in relation to working at home.

1.15.2 University arrangements for home working or 'teleworking' are set out on the Personnel Services website: http://www.admin.ox.ac.uk/personnel/during/flexible/homeworking/

1.15.3 The Novell NetStorage system allows MSD IT users web-based access to their Novell network drives from anywhere in the world via a web browser and internet connection. Users working on sensitive and confidential data should ensure that local copies are deleted or saved on encrypted drives at home. See http://www.imsu.ox.ac.uk/content/novell-netstorage

1.15.4 An alternative approach for Windows users only is *iFolder* (http://www.imsu.ox.ac.uk/content/ifolder) which automates file synchronisation between home and work computers and the iFolder server. This means that you always have access to the most up-to-date copy of a document on all machines.

1.15.5 The University's VPN service allows full access to the MSD IT servers via a Novell client as if they were on the University network. Users working on sensitive and confidential data should ensure that local copies are ether deleted or saved on encrypted drives at home.

1.15.6 The VPN service does not give access to users' personal computers even if they have enabled file sharing (which will only work within the local subnet, i.e. IP addresses 129.67.4.0/22). Special 'remote desktop' provisions can be made with MSD IT – contact the IT Officer for further details.

1.15.7 Home working which involves taking a computer or data drive home will be subject to risk assessments and appropriate steps to mitigate risk will be applied. In such cases hardware and software will be provided by the University and this will be covered by the University Insurance subject to an excess of £2000.

1.15.8 Where a University computer or data drive is taken home or away from NDCLS (e.g. abroad or to a conference), it will be configured with the University's whole disk encryption system or an approved alternative if WDE is unavailable or unsuitable (e.g. Apple FileVault).

1.15.9 Access to University Nexus email from computers outside the NDCLS premises should be via the Outlook Web Access (OWA) browser interface to avoid local caching of work emails, unless the machine is encrypted.

1.15.10 Downloaded attachments and sensitive documents and files should be saved on an external encrypted USB drive. Encrypted USB 'sticks' should only be used for the temporary transportation of data and not for long-term storage of sensitive documents.

1.16 Mobile Devices

1.16.1 Access to University email services using a mobile phone, tablet or similar device is subject to security risks. Such devices have little or no security. Users are reminded that confidential or sensitive data may be present on their personal mobile device and they must ensure that such data is protected. Minimum precautions include an access lock on the device. University policy is described here: http://www.it.ox.ac.uk/policies-and-guidelines/is-toolkit/mobile-security-smartphones-tablets

1.16.2 Mobile devices accessing the University email system will retain a copy of emails ("caching"). Apart from such emails no sensitive or confidential data must be stored or transferred using a mobile device.

1.16.3 You are strongly advised to configure your University email account on your mobile device as an Exchange *ActiveSync* account, rather than IMAP or POP. As well as optimum performance, it will allow remote device wipe in the event of its loss.

1.16.4 In the event of a mobile device with an active University email account being lost or stolen the IT Officer must be informed immediately who will assist in mitigating the security risks by arranging remote device wipe if this is possible. In any case the device should be blocked from further access using the Nexus OWA email interface and a change of Remote Access and SSO passwords.

1.16.5 Most smartphone operating systems including iOS (iPhone), Android, Windows Phone and Blackberry can remotely wipe your device data in the event of a loss or theft. You are advised to familiarise yourself with the security settings and remote wipe procedures for your mobile device.

1.17 Internet and Cloud services

1.17.1 Users should be aware that internet services provided by third parties may not be located in the EU and may be subject to the laws and regulations of other legal jurisdictions (or none at all) and therefore not secure. Such services include web email providers, e.g. *Gmail, Hotmail, Yahoo Mail, Outlook.com*; document storage and sharing, e.g. *Google Docs, SharePoint Online, DropBox, SkyDrive, Office 365*; and bibliography services, e.g. *EndNote Web*.

1.17.2 Security issues arise as these services are targets for hacking, you don't know who holds your data and data may be unavailable or lost. For example, web email providers automatically scan emails to add context-sensitive advertisements to them. They also have the ability to combine information contained in a person's email messages with information from internet searches.

1.17.3 The University provides many such services which should be used in preference to third parties. These include email (Nexus – http://nexus.ox.ac.uk/), large file sharing (OxFile - https://oxfile.ox.ac.uk), document sharing and collaboration (SharePoint – https://sharepoint.nexus.ox.ac.uk; Weblearn – https://weblearn.ox.ac.uk) and a 'private cloud' (SIS – http://www.it.ox.ac.uk/nsms/private-cloud).

1.18 Building Security

1.18.1 All staff will be issued with Oxford University Hospitals ("OUH") Trust ID cards, key fobs and keys that are appropriate to their level of work. Staff are responsible for their ID cards, key fobs and keys and must notify the Senior Administrator immediately in the event of loss. Staff must not share or give keys and swipe cards to any third parties.

1.18.2 It is OUH Trust ("the Trust") policy that their ID cards should be carried at all times, preferably worn prominently, to facilitate identification of authorised persons on the premises.

1.18.3 Internal offices must be locked independently when not in use and offices that are involved in processing sensitive data will be subject to greater security processes, which should be detailed in an individual project policy e.g. Tissue Bank storage areas

1.18.4 It is advisable that you also secure ('lock') your computer with a password when leaving your office and do not leave items such as laptops, papers and USB sticks on display.

1.19 Information Handling

1.19.1 All staff are bound to the University confidentiality agreement by their employment contract. A copy of their contract will be given to staff when they commence employment. Staff are expected to comply with this agreement at all times.

1.19.2 All visitors are bound to the University confidentiality agreement by the Visitors Agreement which they must sign before coming to in Nuffield Division of Clinical Laboratory Sciences. A copy of their Visitors Agreement will be given to visitors during their induction meeting. Visitors are expected to comply with this agreement at all times.

1.19.3 The confidentiality agreement is enforceable in respect of both electronic and hard copy data files. Staff and visitors are expected to observe due diligence and care when handling and processing paper documents, computer files, electronic records, CDs, DVDs, disks drives, USB sticks or any other storage or processing medium.

1.19.4 All staff dealing with Personnel data are required to undertake training in relation to the Data Protection Act 1998, before access to Personnel data is authorised.

1.19.5 To comply with the Quality Assurance Agency for Higher Education ("QAA") requirements to ensure *"rigour, probity and fairness and with due regard for security"*, candidate numbers and identifiable examination results are designated as sensitive for the purposes of this policy.

1.19.6 All projects will be subjected to a formal risk assessment which will include information and data handling. If appropriate to the nature of the project Information Handling Standard Operating Procedures ("SOPs") will be provided and will be expected to be followed.

1.19.7 Computer screens containing sensitive information should not visible to others. Computers must be secured ('locked') with a password when the authorised user is away from the computer.

1.19.8 Any confidential or sensitive data shall only be transferred using an encrypted media e.g. encrypted USB drive. It is permitted to use an unencrypted drive to transfer data within the premises but the data should be immediately deleted from the media following transfer.

1.19.9 Any computer taken off site with confidential or sensitive data shall be configured with whole disk encryption. See 1.15.8.

1.19.10 Shredders are provided for the secure disposal of any hardcopy work that requires disposal.

1.19.11 Computers, mobile devices, CDs, DVDs, disk drives, USB stick or any other storage or processing medium that require disposal should be returned to the IT Officer for secure disposal according to the University's policy for computer disposal: http://www.it.ox.ac.uk/policies-and-guidelines/computer-disposal

1.20 Exceptional security

1.20.1 If any activity requires a separate security policy, for example storage of clinical data, it will be deemed to be “exceptional” and provision will be made to ensure that the data is secured appropriately.

1.20.2 Users must note that NHS Trusts are the Data Controllers under the Data Protection Act 1998 for data relating to their patients. The Oxford University Hospitals NHS Trust has stipulated that patient-identifiable data (e.g. non-anonymised scans of histopathology slides) may be held only on Trust devices connected to the Trust's network, and that any exceptions to this must be agreed beforehand with the Trust's Caldicott Guardian. Further guidance on the use of patient-identifiable data and research is available here: http://www.oxfordhealth.nhs.uk/resources/2012/08/Integrated-Information-Governance-Policy-V4.pdf

1.20.3 The Information Security Manager will be responsible for ensuring that the specific security policy will be written, implemented, reviewed and tested.

1.20.4 Staff must ensure that all data handling activities are risk assessed and any exceptional requirements are notified to the IT Officer or Information Security Manager.

1.21 Disaster Recovery and Business Continuity

1.21.1 Nuffield Division of Clinical Laboratory Sciences has a disaster recovery plan in place and a risk assessment is in place, which is part of the Nuffield Division of Clinical Laboratory Sciences Risk Register. Business continuity planning forms part of that plan.

1.22 Sanctions

1.22.1 Suspected breaches of any part of the Information Security Policy and related policies should in the first instance be reported to the line manager of the staff member concerned.

1.22.2 All breaches and incidents should also be reported to the IT Officer and Information Security Manager. Incidents that are deemed to be serious will then be reported to the Committee. A log of breaches will be kept by the IT Officer. Thefts must be reported to the police and a crime number recorded. Loss of sensitive data must be reported to the University’s Data Protection team (data.protection@admin.ox.ac.uk) and the Information Security Team (infosec@it.ox.ac.uk).

1.22.3 Any member of staff who is deemed to have deliberately or maliciously breached Information Security Policy will be subject to the appropriate Human Resources Policy sanctions.

1.23 Risk Assessment

1.23.1 Nuffield Division of Clinical Laboratory Sciences have an up to date Risk Register and Asset Register. All projects handling sensitive data will have to have completed and recorded a risk assessment.

1.23.2 The Committee must be notified of any significant risks identified in a risk assessment and plans should be put in place for appropriate mitigation.

1.24 Supervening Policies and References

1.24.1 **JANET Policies**
Users are required to abide the JANET Acceptable Use Policy. Current policies are detailed in full on the https://community.jisc.ac.uk/library/acceptable-use-policy website.

1.24.2 **University of Oxford Policies**
Users are required to abide by any University of Oxford IT and Information Security Policies that are in place. Current policies are detailed in full on the http://www.it.ox.ac.uk/infosec/ website.

1.24.3 **MSD IT Policies**
MSD IT have an additional set of Policies and SOPs that must be conformed to. The current policies are detailed on http://www.imsu.ox.ac.uk/content/msd-it-services-security-policy

1.25 Further information

The Information Commissioner's Office Guide to data protection may be found at https://ico.org.uk/for-organisations/guide-to-data-protection/

MSD IT High Compliance System: http://www.imsu.ox.ac.uk/content/high-compliance-system

IT Services OxFile: http://help.it.ox.ac.uk/services/oxfile/index

MSD IT NetStorage: http://www.imsu.ox.ac.uk/content/novell-netstorage

MSD IT iFolder: http://www.imsu.ox.ac.uk/content/ifolder

Encrypted USB data drives: http://www.imsu.ox.ac.uk/content/encryption-services

Securing mobile devices: http://www.it.ox.ac.uk/policies-and-guidelines/is-toolkit/mobile-security-smartphones-tablets

Mobile device encryption: http://www.imsu.ox.ac.uk/content/encryption-faq#mobile_encrypt

E-mail attachment encryption: http://www.imsu.ox.ac.uk/content/encryption-faq#email_encrypt