IG02: NDORMS Information Security Guidelines

Purpose: This document provides a baseline for understanding good information security practice for members of NDORMS, including important rules they need to follow.

- This document is broken into short sections
- Key points are highlighted at the top of each section
- Further information and links are provided
- If you have further information security questions– for example, around acquisition, processing and storage of data – please contact the Information Governance Manager (infogov@ndorms.ox.ac.uk)

As a member of NDORMS, you have access to all sorts of information. It might be patient details including medical conditions, financial or personnel records or large volumes of lab-generated data. Even having a University Single Sign On (SSO) account and email address means you hold information, such as passwords, which must be carefully looked after.

Information Security is the collection of rules and guidelines that help ensure NDORMS provides the necessary confidentiality, integrity and availability for each source of data it holds.

You work under **national legislation**, such as the Data Protection Act (1998)[1] and the Computer Misuse Act (1990)[2]. You may have additional stipulations because of the nature of the material you are working with. You also need to be aware of the rules of the University of Oxford. A detailed list of the **IT rules** can be found on the IT Services website[3] but there is also a more colourful portal for **Information Security information**[4], including videos and straightforward user guides.

This document is intended to give you a starting point for working within these rules. NDORMS carries out a diverse range of work so please also regularly review local practice with your immediate colleagues and contact the departmental *Information Governance Manager* if you have further questions or concerns. For IT support, contact: Pete Salmond <it@ndorms.ox.ac.uk> (Botnar IT Support Manager) or Alex Wong <alexander.wong@kennedy.ox.ac.uk> (Kennedy IT Manager).

Wulf Forrester-Barker
Information Governance Manager
infogov@ndorms.ox.ac.uk
2 February 2017

[1] In a nutshell, you must protect personal information about living individuals.
[2] Likewise, you must not use computers to cause harm to others, such as installing malicious software.
[3] https://www.it.ox.ac.uk/rules
[4] https://www.infosec.ox.ac.uk/

Contents

Backups

- Ensure your data is backed up and contact the Information Governance Manager (infogov@ndorms.ox.ac.uk) or IT staff if you need support with this.
- Backups protect you against information loss
- Different types of data will require different backup strategies
- A backup is only safe if you know you can restore your data from it

Backups provide a strong defense against information loss. Data recovery may be impossible or prohibitively expensive from a broken device but having recent copies of your information allows you to get back to work quickly.

In most cases, the best location to store your files is not on your computer but on the network. On the network, automatic backup happens nightly. There may be circumstances in which this is not suitable, particularly if you are dealing with sensitive, identifiable data or with very large volumes of data. In some cases, it may be appropriate to make use of the University-provided HFS system or an external storage device. If the data is sensitive, the backup version should also be protected.

Please seek advice from IT or Information Governance staff if you will not be using network storage or if the requirements are otherwise complex.

See also the sections on cloud services and mobile devices.

Further reading:

http://help.it.ox.ac.uk/hfs/index

Cloud Services

- Don't use non-University cloud services for University data without written approval from the Information Governance Manager (infogov@ndorms.ox.ac.uk)
- Convenience has to be balanced against security concerns
- Not everything that is possible is permissible because you can't enter into a contract on behalf of the University
- Always consider University-based alternatives

Cloud services – including well-known services like Dropbox or Google Drive – are sometimes referred to as "your data on someone else's computer". They are convenient but not always suitable because they put copies of your data in places you have no control over. Additionally, services often require agreeing to the provider's terms and conditions and you can't enter into a contract on behalf of the University. You cannot guarantee that no-one else has stolen a copy of the data or that, on deletion, the information is removed from all servers it was stored on.

In many cases, there are University provided services that will provide an equivalent or better solution. For example, you can use the University's Virtual Private Network (VPN) to access your network drives from home and there is also a VPN service run from the Kennedy. This also avoids keeping a copy of files on non-University machines and offers other benefits, such as allowing you access to online journals as if you were sitting within the University. You should only use trusted machines for this which are protected by anti-virus software and up to date with security patches. If you need to send or receive large files, Oxfile can deal with files up to 25GB in size. Check with IT staff for help with these locally-provided services.

Further reading:

https://www.infosec.ox.ac.uk/i-want/use-cloud-services-safely

https://www.infosec.ox.ac.uk/want/secure-accounts

http://help.it.ox.ac.uk/network/vpn/index

https://oxfile.ox.ac.uk/

Email

- Contact IT Support if you encounter a virus or the Information Governance Manager for phishing messages that appear to come from the University (infogov@ndorms.ox.ac.uk)
- Email is widely used but is insecure without taking uncommon precautions
- You can't unsend an email so consider before you commit to it
- Be cautious about the content of emails you receive

When sending emails, you should be careful about the written record you are creating. When including people in an ongoing email conversation, it may be sensible to remove older messages to keep the discussion appropriate to the new scope. You should also consider how aware the recipients are of each other; often it is useful to understand who else is in the group but if, for example, sending out a newsletter, do you have permission to give each recipient the email address for everyone else involved? Once the email has been sent, it has gone outside your control and could end up forwarded and stored on systems you would not consider trustworthy.

When you receive emails, you will get a certain amount of spam – unsolicited marketing material and other junk. The University spam filters reduce the amount you see but, to avoid important messages getting lost, are set not to be too zealous. If you see an email that tries to impel or entice you to click on a link, be very cautious. This may be what is known as 'phishing' and this class of spam has become quite hard to spot. Watch for signs like a sense of urgency or a link that is complex or shows a different address when you hover over it. Please advise the Information Governance Manager of phishing messages that pretend to come from the University of Oxford; other phishing attempts can be deleted.

You should also be cautious of attached files. If unexpected, treat with caution even if they appear to come from a trusted source. If you realise you have been caught out, disconnect from the network and then contact local IT support to arrange immediate assistance. They will help you disinfect your computer and will provide the necessary report to the OxCERT security team.

Do not keep sensitive personal information such as shortlisting files in your email any longer than necessary as this is another copy of the data. Where possible, find other ways of sharing and receiving such information.

Further reading:

https://www.infosec.ox.ac.uk/want/phishing

https://www.infosec.ox.ac.uk/want/email-securely

Encryption

- Mobile devices containing personal data, including phones and laptops, should be encrypted
- Encryption offers very strong data protection
- There are different ways to use encryption
- Depending on your work, there may be situations where it is a definite requirement

Encryption jumbles data so that it can only be unlocked by providing a key, often in the form of a password. There are many ways things can be encrypted but, if you use a reputable method, the main risks to your data are either that someone steals your key or that you forget it!

Encryption can be applied at various levels. You can protect an individual file if the application lets you set a password. Microsoft Office products since Office 2007 provide very strong protection and you should be using at least Office 2010 for your work. For password options in other programs you will need to do some research or check with IT staff. You can also use software to protect a folder or create an encrypted file that opens up like plugging in an external drive. Veracrypt is a good cross-platform tool and there are also Operating System (OS) specific tools (eg. Bitlocker or 7-zip for Windows; FileVault for Mac).

You can even encrypt a whole device. This can be done with OS tools or the University provides a free Whole Disk Encryption service which IT staff can assist you with. The advantages of this are that the encryption of your system is registered and authorised staff can access a master key if you lock yourself out! It doesn't protect against all risks — for example, while the machine is running you are still relying on the screenlock password — but it does become significantly better protected. Encryption can also be applied to external drives; you can request a USB stick with hardware-based encryption from IT staff if approved by your PI or manager.

When you use websites with URLs beginning HTTPS, indicated in most browsers with a padlock icon, information is automatically encrypted between you and the server at the other end. This is important when sending or receiving secure information, including logging in to a system with your username and password. Encryption is also recommended when you keep sensitive data on a Solid State Drive (used in many recent machines for speed improvements over Hard Disk Drives) as previous secure deletion techniques, short of physical destruction, are no longer certain to work.

Further reading:

http://help.it.ox.ac.uk/wde/index

http://veracrypt.codeplex.com/

Location and Being Overlooked

- Be aware of your surroundings
- Not all networks are trustworthy
- Avoid your screen being overlooked by unauthorised people

Mobile devices and cloud services give you freedom to access information in many places other than your office. You should be aware of the additional risks this poses.

When accessing websites and data, you are sending and receiving messages across network connections. Where possible, it is sensible to use secure websites, which will have addresses starting https:// rather than http:// as these automatically encrypt your communication with the site. From networks you cannot

confidently trust, such as hotel and airport Wi-Fi hotspots, use the University's Virtual Private Network (VPN) software to provide a secure tunnel into the Oxford network; this also has the advantage of giving you access to many journals and other services the University subscribes to.

In public places, you should be appropriately cautious about what devices you are seen to be using to avoid becoming a target for thieves. This applies to the risk of somebody stealing your device but also the possibility of someone reading or photographing your screen.

In any location, do consider whether your screen and keyboard are overlooked, for example through nearby windows. You may need to take preventative measures and should certainly lock your screen when you leave it unattended. Even in NDORMS buildings, be careful about security and take measures such as shutting windows when you leave a room empty and reporting if you lose your card.

Further reading:

http://help.it.ox.ac.uk/network/vpn/index

Mobile Devices

- Seek advice from the Information Governance Manager (infogov@ndorms.ox.ac.uk) if unsure what applies to your devices and data.
- Not all data is allowed to be carried on portable devices
- When you can use mobile devices, take additional precautions to protect the data from loss or damage

Mobile computing and storage devices (laptops, USB / memory sticks, smart phones, tablets, etc) are relatively high risk, because they can be easily lost or stolen. It is essential that such devices are properly secured. In many cases, some form of whole disk encryption (see the section on encryption) is appropriate.

You should be aware of what information is held on each of your mobile devices. Where possible, it is sensible to avoid carrying sensitive information around but this can be difficult. For example, if you run an email program, this probably keeps a copy of the messages on your local drive. If you check your emails from a phone or tablet and only use a short PIN or pattern, that is the only protection you have keeping your account safe.

Some of the arrangements under which we collect and hold data will either insist that your devices are encrypted or require that you must not use mobile systems to work on the data. While this may seem inconvenient, it is essential that you understand and follow the rules that apply to the data you are working on.

Further reading:

https://www.infosec.ox.ac.uk/want/mobile

Passwords

- Passwords should be at least 12 characters long and use more than one type of character
- Longer passwords are stronger
- Don't write your passwords down but do find software or other systems to help manage them

For many systems, a password is still the first line of defense. Each password should be long and reasonably complex. Use at least 12 characters and preferably 15 or more. You should also include some

mix of upper and lower case letters, numbers and symbols; this ensures hackers have to use the widest possible character set to build their guesses.

You may find it helps to think in terms of shorter chunks – for example, three sets of five characters. Make sure you can type your passwords accurately, finding patterns that fall under your fingers – but avoid simple runs of characters from the keyboard, like qwerty123456. Using numbers and symbols to stand in for $imilar characters is of limited value because it is hard to remember which ones you chose but easy for a hacker to create a 'dictionary' including common substitutions.

You should use different passwords for different systems and change them periodically. Central university systems require a yearly change. More frequent changes do not necessarily increase your security but may be required by particular systems you connect to. You must not write your passwords down in plain text but may find it useful to investigate password management software and systems such as LastPass and KeePass. You should also not share your password with others or allow them to access resources under your account.

Do look online for further advice about common passwords you should avoid and how to create strong passwords but don't copy any of the examples you find directly as these are also likely guesses for hackers.

Further reading:

https://www.infosec.ox.ac.uk/strong-passwords

https://xkcd.com/936/

Protecting Your Computer

- IT staff can assist with physical and software security
- At least lock your screen before leaving your computer unattended
- Use physical security to stop thieves being able to get to and take away your devices
- Apply software security updates and keep antivirus software running

You must take reasonable steps to protect the computers you use. For example, lock the screen before walking away from the device even if you anticipate that you will only be gone for a minute (Windows: Windows key + L; Mac: set up a "hot corner" to activate the screensaver). It is recommended that you shut down your computer down at the end of the day unless you need to run an overnight job. If that is a frequent occurrence, it would be sensible to consider an Uninterruptible Power Supply (UPS) device to protect against problems from unscheduled power cuts.

Physical security should be considered. Portable devices should be either be shackled in place or locked away when left unattended. Locks should be used when rooms or furniture is not in use; open plan offices should not be assumed to be secure. Confidential data should be kept under lock and key when not in use. A safe is being installed in the Botnar to hold drives with encrypted contents so that we can monitor where they are when not in active use (contact infogov@ndorms.ox.ac.uk for details).

Software security should be maintained. If you can install software on your machine you should only do so from reputable sources. They should be updated with patches and you should remove programs you installed but no longer use. You should also have modern antivirus software (Sophos by default, unless you have arranged with IT staff to use an alternative) running on your machine. See also the section about software and downloads.

Further reading:
https://www.infosec.ox.ac.uk/protect-devices

Reporting Issues

The following types of security incident should be reported immediately to **local IT staff**, who will assist and also inform the Information Governance Manager (infogov@ndorms.ox.ac.uk) and central OxCERT team:

- Lost or stolen devices
- Malware infections
- Suspected hacking or unauthorised access
- Unintentionally emailing sensitive information to the wrong recipient

Suspected incidents should also be reported for investigation. For example, you may suspect hacking if you see a departmental website with odd advertising links, or unauthorised access, if you find your computer switched on when you are sure you turned it off the night before. The department is required to keep a record of security incidents and co-operate with other University teams.

You do not need to report viruses that are blocked or 'Potentially Unwanted Programs' your antivirus software picks up but may wish to discuss with IT staff to find ways to avoid more serious problems in future. If you are not sure about whether an email contains a phishing link or malware, do check with colleagues or refer to the Information Governance Manager (see the section on email).

Further reading:
https://www.infosec.ox.ac.uk/report-incident

Research Data

- Holdings of research data should be registered with the Information Governance Manager (infogov@ndorms.ox.ac.uk) on the NDORMS Information Asset Register
- Research data is highly precious and should be treated as such, including paper-based as well as electronic material
- We must observe all the requirements made in order to lawfully collect it
- A data breach could have significant financial cost and long-term reputational damage to the department and University

Data held for research projects may have extra stipulations in order to ensure that we are operating in a legal manner and fulfilling any contractual obligations. Many funders now insist on data management plans being drawn up as part of the application but this is recommended as worthwhile documentation for all research projects; if your data is important enough to use, it is not too trivial to benefit from a plan.

Your plan should indicate what data you plan to hold or collect, where it will be stored and who will have access to it. You should also consider the size of the data including rate of growth, any particular sensitivities and how you will mitigate the risks, and what will be done with the data at the end of the project or if other groups ask to share it. Research data holdings should be registered with the Information Governance Manager (infogov@ndorms.ox.ac.uk).

You must adhere to promises you made in securing access to the data, including secure deletion of the material and any backups if it must be purged at some point. Deletion should be witnessed by the

Information Governance Manager, but planning should begin early, before copies and back-ups get spread around.

Further reading:

https://www.infosec.ox.ac.uk/i-want/secure-my-research-data

Software and Downloads

- If unsure about software and downloads, please check with IT staff
- You must make responsible use of your network connection
- You must not download illegal material

Accessing the University network or being able to install software is a privileged position. You should only install software from reputable sources and ensure that they make responsible use of the network. Many research resources require the use of streaming media services such as YouTube. However, the department and the University as a whole only has finite bandwidth to share among all users so it is not appropriate, for example, to spend all day listening to Internet-based radio services.

You should also exercise discretion in files you download. Avoid, for example, illegal copies of films and music. Not only does the breach of copyright law mean you have strayed beyond acceptable use of the academic network but the sources for this material are often infected with malware – the criminal profits from this may be how the material is funded in the first place. This would also apply to files you have downloaded on a personal connection but transferred to a University machine.

Network traffic is monitored by the University. Although care is taken not to infringe your rights, there are records that could be traced to you so remember your accountability and responsibility when making decisions about what to bring inside the work network. If you need to handle potentially illegal material as part of your work, the guiding principle is that you must get explicit permission first!

Further reading:

http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

https://www.it.ox.ac.uk/policies-and-guidelines/handling-illegal-material

Working From Home

NDORMS actively supports flexible working practices, including arrangements to work from home. This is often convenient and, in most cases, technologically feasible. However, you should also consider the information security risks of this approach.

If working online, you should consider using a University VPN service. IT staff can explain how to set this up. It will give you secure access to 'Oxford only' resources, including files stored on network drive and access to many online journals. You should protect the computer you work on by keeping software up to date and running antivirus software – you are entitled to run a copy of Sophos on your home computer.

However, this flexibility creates many additional risks. First you should check within your team or by contacting infogov@ndorms.ox.ac.uk that accessing the information at home is permissible. If you are not using a VPN service but physically carrying the data, how is it protected from loss or damage enroute? Once safely home, can you store and use the data without others being able to see or access it? Is your home Wi-Fi secure – at very least, not using the default password?

As you are working outside of the supported environment of the department, you carry more responsibility for the security of your information. In this guide, pay particular attention to the sections on **Location and Being Overlooked**, **Protecting Your Computer** and **Encryption**.

Further reading:

https://www.ndorms.ox.ac.uk/about/working-with-us/work-life-balance

http://help.it.ox.ac.uk/network/vpn/index

http://help.it.ox.ac.uk/viruses/index

Document History

Version	Authorship	Key Changes	Date	Review By
1.0	Wulf Forrester-Barker NDORMS Information Governance Manager	First published version	2 February 2017	April 2018