Information Security and Governance at NDORMS

Each person in NDORMS has a responsibility to contribute to the appropriate confidentiality, integrity and availability of our information resources. You must follow NDORMS and University rules and work within national data protection legislation including GDPR.

Information security is about protecting data from damage or misuse. That includes malicious attacks and theft but also other problems, such as accidentally deleting a file, sending a sensitive email to the wrong recipients or experiencing a computer failure. Our Information Security Policy details a number of things you need to know to use your data resources safely.

Information governance relates to the collection of policies, processes and monitoring that ensure we maintain suitably high standards of information security.

What do I need to do?
There are three things you must do during your induction period:

1. Read the NDORMS Information Security Policy (IG01) and Guidelines (IG02). See: http://www.ndorms.ox.ac.uk/information-security-policy
2. Find out from your immediate colleagues about specific security and governance requirements for the information your team works with.
3. Work through the University's online information security module, available at: https://infosec.ox.ac.uk/module/ (estimated time: 15-45 minutes). There is a multiple-choice test at the end and you must score 70% or more although you can retake it. It is recommended that you save a copy of your final test certificate.

When you have completed these tasks, please contact the Information Governance Manager (infogov@ndorms.ox.ac.uk) to confirm this and to ask any further questions you have about information security and governance at NDORMS.

Within your first few weeks you will also be invited to a group information governance induction meeting. This is an opportunity to meet other new starters at NDORMS, learn more about your responsibilities and discuss any IG issues you might have come across in your first few weeks.

Further Tips

- Think about where you put your files and who you are sending emails to.
- Use long passwords (16+ characters) and find a system to help you remember them – consider password managers like Lastpass, Dashlane and KeePass.
- Don't share your login and lock your computer when leaving your desk to protect your identity (Windows-L on a Windows machine).
- Keep an ear out for current threats and be cautious about what you click, as emails and websites can hide malware – you can send 'Oxford' branded phishing messages as attachments to phishing@it.ox.ac.uk but get IT support if you think you've been affected by malware.
- If not saved on the network, make sure your data is backed up and that the backup isn't stored next to the original. Think secure and stay safe.

Lydia Underdown, Information Governance Manager <infogov@ndorms.ox.ac.uk>, May 2019