Version 1
Last amended: 2 July 2015

The University of Nottingham
UNITED KINGDOM · CHINA · MALAYSIA

Guidance Document: New Staff Induction – Records Management Framework

Background
The University already has lots of central guidance and information covering the induction process for new members of staff, in addition to any local induction practices at schools and departments.

Professional Development has a central source of information on their Induction webpages, and workspace pages covering all the key aspects of a solid induction programme. These workspace pages provide links to other relevant webpages and information including:

- Ethical Framework
- Information Security
- Human Resources
- Legal Podcasts
- Equality and Diversity
- Welcome Events

The Records Management Framework has now been added to this list with the intention that important messages around information compliance and data security can be highlighted to staff early on in their induction process. It is designed to set the precedence for how we manage our information assets. It does not replace the need for staff to read key policies, some of which are highlighted throughout this document.

The following text now appears on the workspace 'Legacy and Policy' pages which can be accessed via the Professional Development Induction webpages:

The Records Management Framework

The University is classed as a Public Authority under the terms of the Freedom of Information Act 2000. This means all recorded information may be subject to disclosure either through our Publication Scheme or via Freedom of Information (FOI) requests made to the University by any member of the general public. This includes information recorded in emails.

To raise awareness and promote best practice in how we manage our records and information, we have introduced a Records Management Framework across the University, and nominated Records Officers at each School and Department to act as a local point of contact.

Records Officers will be able to assist you with any queries you may have relating to Records Management and Information Compliance, including FOI and Data Protection. They will also be able to give you about specific Records Management/Information Compliance information relevant to your working area.

As part of your induction process, familiarise yourself with the Records and Information Management Webpages, and book in a meeting with your Records Officer who will talk you through each of these key areas.

- The Records Management Framework
- Data Protection
- Data Security
- Freedom of Information
- Records Management
- Data Breaches

Induction Process
The Records Management Framework induction should be completed by the Records Officer with each new member of staff.

A short meeting will introduce that member of staff to their Records Officer who will be able to run through the following key messages. These key messages can be added to by each School or Department to highlight specific records management practices in each area.

Records Management Framework Induction Checklist

Suggestions are made in *Italics* for additional information you may choose to include.

1. The Records Management Framework	Completed ✓
1.1 Purpose: The Records Management Framework comprises a network of Records Officers who provide an important communications link between Schools and Departments and the Records Management Steering Group. The purpose of the Framework is to raise the profile of records management at the University. Records Officers act as a local point of contact in their areas; they enable issues to be raised and addressed locally and they cascade all policy and guidance updates provided monthly by the Information and Records Manager.	
1.2 How is it organised: The Records Management Framework is managed by the Information and Records Manager who reports into the Records Management Steering Group, chaired by Registrar. There is at least nominated Records Officer at each School and Department who acts as a local point of contact for any records management, information compliance or information security issues. The Records Officer will escalate any issues you may have to Records and Information Manager. *Does your school or department have more than one Records Officer?* Each month relevant updates or guidance documents are cascaded and published on the Records Management Framework webpages. If you have any requests for topics to be covered you can request that they are included in the Framework programme. Previous requests covered include Student Records and Staff Records Guidance. Look at the Records Management webpages and familiarise yourself with the previous guidance cascaded.	

2. Data Protection	Completed ✓
2.1 Overview: The University of Nottingham is a Data Controller under the Data Protection Act 1998. This means we are responsible for handling all personal data held in accordance with the Act. Most staff process personal data in some form or other, whether this is student, staff or third party personal data. It is important that all staff are able to identify when they are processing personal data and are aware of their responsibilities. Breaches of the Data Protection Act can lead to fines of up to £500K and cause considerable reputational damage.	
2.2 Key Messages: Read the following policy and guidance information: University Data Protection Policy Data Protection in the Workplace Do you know how to identify what personal data is? Have you received Data Protection Training? The following training is currently available to all staff: Data Protection Pod briefing (Compulsory for all staff to watch) Essential Data Protection for Staff (monthly staff course for all staff) Talk to your line manager if you think you need further training and include it in your personal objectives for the year. Be aware that the University will not disclose personal data to anyone other than the data subject unless they have prior consent from the data subject concerned. This includes incidences where a parent contacts the University to discuss details about their child. If you are involved in any projects involving the use of Data Processors (third party external companies who process personal data on our behalf) you will need to have in place a Data Processing Agreement. There is a standard agreement in place for all such contracts and you should always consult with the Governance and Information Compliance Team. *What personal data does your school/department process and how is this kept secure?*	

3. Data Security	Completed ✓
3.1 Overview: The University is constantly under threat from malicious individuals and computer programs like viruses and worms. The attackers seek to access IT resources and sensitive or personal information for their own, increasingly criminal, purposes. We are obliged by legislation and our own governance to protect against this. All staff should remain vigilant to possible threats and always report any suspicious activities.	
3.2 Key Messages: The IT security service The IT security service protects the campus network from unauthorised access, data loss, identity theft, damage to computers or network services, and computer viruses. Read their webpages for up to date guidance about how to protect our data assets and stay secure. There are lots of practical ways that staff can contribute to a secure working environment. Here are some of the key points: a. Passwords Never share passwords with colleagues. Never write them down where they can be accessed by others. Use suitable passwords and change them when prompted. Password protect any documents that warrant protection. b. Operate a clear desk policy Don't leave sensitive or confidential material out on display and always lock your computer screen when you are away from your desk. Keep sensitive or confidential records locked away. c. Taking materials off site Don't take sensitive or confidential materials off site unless they you need to and unless they are suitably protected ie password protected d. Mobile devices Don't take sensitive or confidential materials off site on unencrypted memory sticks, tablets or laptops etc. It is possible to access almost everything you have on a University PC on an alternative computer at home. See Working Off Campus e. Be vigilant to hacking attempts and phishing – report anything suspicious Don't open suspicious emails or attachments; report them to the IT Helpdesk. f. Be aware of blagging Always confirm the identity of an individual first before disclosing information to them *Add any additional security measures that are specifically relevant to you working area. For example what is the routine for the last person out of the office? Locking doors, windows, putting on the security alarm etc..*	

4. Freedom of Information	Completed ✓
4.1 Overview: The University is classed as a Public Authority under the terms of the Freedom of Information Act 2000. This means all recorded information may be subject to disclosure either through our Publication Scheme or via Freedom of Information (FOI) requests made to the University by any member of the general public. This includes information recorded in emails.	
4.2 Key Messages: A valid Freedom of Information Request is one which is: • Made in writing • Includes the name and address of the Requestor (does not need to be their real name/can be the name of an organisation) • Describes the Information Requested The University has 20 working days on receipt of a request to comply and provide the information if held, subject to any exemptions. The requestor does not need to state that it is a Freedom of Information Request, so all staff must be able to identify if they receive one and forward it to the Governance and Information Compliance Team. The Governance and Information Compliance team may contact us if they receive a request for information and they believe we hold that information. It is important that we respond quickly stating if we hold the information and if necessary providing them with that information by the date they provide. Requests for information can cover an array of topics and subjects. It is important that we keep all our records and information accurate and up to date so that we can respond promptly and efficiently to all requests received. If you think you have received a request, contact your Records Officer and inform the Governance and Information Compliance Team who will make all necessary acknowledgements and responses. Remember email may be subject to disclosure under a Freedom of Information Request. *What types of information are generally sought from your area under FOI requests? When contacted with an FOI request by the Governance Team, who normally responds to them?*	

5. Records Management	Completed ✓
5.1 Overview: Records Management is about knowing what you've got, where you've got it and how long you need to keep it. The University has centrally accessible services and support to help Schools and Departments manage their records and information, but ultimately it is the responsibility of each School and Department to ensure good records management practices are adopted and followed.	
5.2 Key Messages: <u>Local Records Management Practices</u> Explain to the new staff member key records management practices in your area: • How is your shared drive is organised? How are records filed within your shared drive? Remember not to save University records on your personal drive where they cannot be reached by other staff members who need access to them. • Where you keep paper records? What on site storage facilities do you have? <u>Records Retention</u> The University has a Retention Schedule which is a guide to how long we need to keep certain classes of information. All schools and departments are ultimately responsible for how long they need to keep their own records, and such retention practices should not be inconsistent with the Data Protection Act which states that personal data should not be kept for longer than is necessary. Explain to the new staff member how records are organised and destroyed in accordance with either a local retention policy or the University retention policy. <u>Records Storage Facility</u> The University's Record Storage Facility provides a medium to long term storage solution for Record boxes containing University Records. The service is run centrally for all Schools and Departments (box owners) and is operated by Transport & Logistics, a Division of the Estates Department. Its primary purpose is to provide a secure and accessible depository for the Record boxes until they are recalled by the box owners or reach their destruction date. <u>Confidential Waste Disposal</u> • Only use the paper recycling bins for general waste only (ie not confidential, personal data etc) • Don't put general waste in for confidential shredding. Whilst the confidential waste disposal service is a cost free service to schools and departments it still costs the University as a whole • If you have small volumes of confidential waste shred using your own shredding machine. Where are these situated in your school/department?	

Under the Freedom of Information Act the University needs to comply with the Lord Chancellors Code of Practice for Records Management. If you have any questions around managing University records contact your Records Officer who will then escalate any issues or queries to the Information and Records Manager.	
6. Data Breaches	**Completed** ✓
6.1 Overview: There are many forms of a data breach. Those that are caused by technical error, those that are caused by third parties, those that are caused by malicious attacks and those that are caused through negligence. Data Breaches may involve a variety of data types, including personal data, research data or other confidential data. They may be caused through loss, destruction, deletion, etc.. of electronic data, or physical paper records. The University is currently working to identify how it can best protect from known data breaches and further policy and guidance is due to be published in the near future.	
6.2 Key Messages: If you identify a data breach you should report it straight away. The Governance and Information Compliance Team will need to be aware of the breach so that they can include it on the Data Breach Log. They will be able to offer advice about what steps will need to be taken to minimise the impact caused. The Data Breach Guidance should be read by all new members of staff. The aim of this guidance is to help staff to: 1. identify when a data breach involving personal data has taken place; 2. understand the main causes for data protection breaches, and how these can be minimised; 3. take appropriate action in the event of a data breach occurring involving personal data. The most form of data breaches is via email. Be especially vigilant when sending emails that you have the right recipient. If you identify a data breach out of hours, staff should report it via the IT helpdesk: x16677 *Who in your School or Department will need to be informed in the event of a data breach?* *ie School Manager/Head of Department etc.. Explain what your internal process is for reporting data breaches. Do you have any examples of recent breaches?*	

The University of Nottingham
UNITED KINGDOM · CHINA · MALAYSIA

To be completed by all new staff on completion of their Records Management Framework Induction

Staff Self-Assessment Checklist	Completed ✓
1. I know who my local Records Officer is and have completed the induction checklist with them	
2. I have visited the Governance and Information Compliance webpages and know the key areas of work they do	
3. I am aware of the Data Protection training available at the University and have included this in my objectives for the current year	
4. I know if I handle personal data and have read the University Data Protection Policy	
5. I know that all Data Breaches need to be reported promptly to my Records Officer and the Governance and Information Compliance Team	
6. I understand how records are managed in my area and where they should be kept either in electronic or paper format	
7. I know that Records should be kept in accordance with the University or the local school/department retention schedule	
8. I know how to destroy records confidentially	
9. I know how to identify a Freedom of Information Request (even if it doesn't state it is a Freedom of Information request by the sender)	
10. I understand that data security is vitally important to protect the University from external or malicious attacks, and will follow the best practice guidance provided to stay safe	