Quick Guide

To looking after employee information

Why it matters...

The University is a people business – people are one of our most important assets and essential to the delivery of education and research. As such, many employees will use personal information about people as part of their job.

This Quick Guide explores some of the ways in which employee information can be accessed and top tips to protect it. Remember – we are all employees so we are talking about your information and your privacy here as well!

How it works

I am the reporting manager - what do I need to do?

1. Responsibilities

As a **Reporting Manager**, you have a responsibility to support and manage one or more employees and to recruit and select prospective employees. To help you undertake these responsibilities you will have access to personal and employment details.

You need to access this information in order to be an effective and efficient manager, but there is an obligation on you to

- use the information appropriately to the task in hand;
- share it wisely;
- protect it from misuse;
- store it in accordance with University policy.

As an **employee**, you may also be required to review the personal and employment information of staff, in order to carry out your duties. For example, you may have to

- check data sets for accuracy;
- review lists of staff to consider the allocation and the deployment of resource;

- ensure employee entitlements and services match status;
- analyse employment trends and employee achievements.

The information you access to carry out your role can be made available to you in a number of ways. Below we review the principal ways in which information will be provided and how it should be safeguarded.

2. Accessing information in University systems

The University provides as much relevant information as it can electronically within its corporate information systems (e.g.Agresso for finance, iiTrent for human resources). In such systems you will be:

- set up as a user, with privileges appropriate to your role and seniority.
- Guided through the completion of transactions with the appropriate level of detail and data to hand.
- Working within the parameters of existing business rules, eg for reporting manager relationships
- Protected from allegations of misuse through the logging of access and transactions on your user name.
- Supported with system infrastructure for the archiving and disposal of redundant records.

Despite these safeguards there are still some key points to implement:

- Log out of any system when you no longer using it.
- Protect your login details. Never share them – this compromises your protection from allegations of misuse as much as it compromises the actual data.
- Report any local changes in your duties to the relevant system managers, if it means that you no longer require certain levels of access.
- Try not to screen shot anything unless you are sending it to an employee that you know has the same level of access to the information.

Of course, as soon as you extract information from as system it is no longer protected by the system infrastructure. Next, we review handling employee information outside our secure systems

3. Accessing Other Sources of Information

You may handle the following sorts of information outside the University's corporate systems, typically in emails and shared drive or online resources, even if the information has originated from a system:

- personal and employment information sent to you in emails or as attachments e.g. spreadsheets

- application forms and documents from prospective employees that have been printed;
- Right to Work documents for verification;
- Fit Notes;
- Procedural documents: grievance, disciplinary, conduct, Permanency & Probation, Annual Review etc;
- Committee minutes with records of staffing decisions.

Because such information is not protected by system protocols it needs careful handling. See the box on the right for guidance on safeguarding information outside our secure system.

4. Security Guidance

In addition to the basic security principles you should:

- Tell anyone sending you information regularly if you no longer require it, so they can update any distribution lists.
- Think-before-you-forward. Does the recipient need the whole attachment or content of the original email?
- Double check the recipient(s) before you send email. Ideally, find a way to share large amounts of personal information that doesn't include email.
- Be careful about how you connect your University email account to a mobile device. How do you protect the device? Ask your manager for a specific device if your work requires extensive remote working.
- Be careful about using unsecured wi-fi.
- Understand the status of information that you have – is it a copy of an original? Are you responsible for archiving or destruction.
- Consider your use of shared drives. Do you need a new share or subfolders with different levels of access.
- Never send a USB in the post. Protect it with passwords.
- Do not read hard copy or screen-based information in public places.
- Carry hard copies securely if working at home and keep safe at home.
- Don't leave things on printers in common areas. Use the job-release function on shared printers, where a pin code is used to release your work
- Avoid conversations about employees in corridors, catering and retail outlets, public spaces and open plan offices.

Contact Develop@essex.ac.uk for support. For more Quick Guides go to the webpage.