UNIVERSITY OF Southampton

Policy

Title:	**DATA PROTECTION**
Ref:	HR/RT **Last updated:** 1 June 2010

1. Security of staff information

1.1. Introduction

This policy outlines the steps to be taken to ensure security of payroll and personal information relating to all staff employed by the University and the release of personal information relating to an employee to internal/external individuals/organisations. This policy applies to those who have access to any personal information and to all users of the Personnel Information Systems, Profund (Superannuation), Compel and systems which download from these. This policy will ensure the University complies with the Data Protection Directive.

1.2 Scope

The purpose is to identify rules to prevent unauthorised access to payroll and personal information (relating to staff) held manually and on computer in personnel, payroll and in individual departments and to give staff access to data held about them. This policy is subservient to the Data Protection Act/Data Protection Directive and users must be aware of their responsibilities under the Act/Directive to ensure their compliance. Heads of School should make users aware of their duties and responsibilities.

There are only three permissible hard copy (paper) files relating to employees: the formal personal record held in Human Resources; the payroll file in Payroll Services Office (including any pension files) and the departmental file held by the relevant Head of School.

All employees have the right to access information held about them on these and any supporting computer files and to insist on the correction or removal of inaccurate material, therefore, procedures should be in place to ensure that information is relevant and held in a secure manner.

1.3 Data Protection Directive

The Data Protection Directive covers all files that are manual or computerised that are identifiable by a personal factor, ie., staff number or name.

The Directive applies to data held in a 'relevant' filing system, which should be structured. This covers all computerised and manual systems including local text and data processing applications.

2. Computer information concerning employees

2.1 Access to the system

A User's Head of School must authorise access to the system by completion of a user request for the Payroll and Personnel Information systems. These forms will detail the level of access a user is given, and confirms that the user will have responsibilities under the Data Protection Act made clear to them and that they will receive adequate training in operating the system.

2.2 Password security

Users are made aware that their system password is the equivalent of their signature and that they must not divulge their password to others, nor must they seek other user's passwords. If their password has become known by another, they must change it immediately.

2.3 Viewing of data

Steps must be taken to avoid accidental disclosure of information to visitors and other non-authorised users in the users' department. If a visitor to the department who is not authorised to see personal information is present, computer screens should be switched off or switched to another programme. Note that it is not necessary to switch the computer off. If the user is leaving the room, they should log off the system completely.

2.4 Information held on computer memory or storage discs

Information obtained from the personnel or payroll system, but stored in other files must be password protected to prevent unauthorised access. Storage discs should be stored in lockable boxes.

2.5 Payroll department paper files

All employees of the University will have a personal file which will contain some information already held by Personnel and other personal data as supplied by the Inland Revenue; Department of Social Security; other Government Agencies and Statutory Bodies; Trades Unions; Pensions Schemes; Banks and Building Societies; University departments, and the relevant employee. Each file will be noted on the front with the employee's name and pay reference. All information contained within an employee's file will be held in date order.

- A range of information will be held within each personal file and may include:
- A copy of the signed contract of employment
- A personal details form
- Tax forms P45 or P46 sent to HMIT unless held because pay is below threshold
- Tax forms P6 (as periodically amended)
- Pension scheme option forms
- Voluntary deduction mandates
- Changes in bank details
- Details of ad hoc payments
- Pension scheme beneficiary options
- Court orders
- Child Support Agency orders
- Attachment of earnings orders
- Telephone reimbursement claims
- Copies of Contributions Agency enquiry forms
- Solicitors enquires - re accidents
- Jury service claims
- Long term periods of sickness (over 4 days)
- Death in service correspondence with legal representatives
- Paid up FSSU Insurance policies

Personal files relating to staff who leave the University will eventually be micro-filmed and the original documents destroyed.

2.6 Departmental paper records

Departments may keep locally held paper records relating to individual staff employed in the particular department. Such files should be known to and open to access by the appropriate Head of School and HR Adviser. While departmental files do not have the same formal status as the prime Personnel or payroll files, they are included in the scope of the Data Protection Act, 1998. The departmental employee file may include departmental copies of authorities, eg any authorisation to advertise the post, local correspondence relating to employment matters resolved without need of recourse to Human Resources or formal University procedures, copies of any appraisal records, annual leave or sickness records, copies of expenses claim

forms, etc. The departmental employee file may also contain duplicates or sub-sets of Human Resources or Payroll Services files.

2.7 Storage of paper files

All Human Resources, Payroll or department files should be stored in lockable cabinets/storerooms and filed in alphabetical order. Only authorised personnel will have access to employee files as determined by the Personnel, Payroll or Superannuation Officer. Personal files will not be removed from the department without prior consent from the responsible Officer. If any personal or departmental file concerning a named employee is believed to be lost the Director of Human Resources will be notified immediately.

2.8 Clear desk policy

Due to the confidential nature of the work of Human Resources and the information held on employees by Heads of Schools, the University supports a clear desk policy. At the end of the working day, all personnel files and other confidential information regarding employees of the University should be removed from the desk to a lockable drawer/cabinet/storeroom to ensure security of information which could be identifiable to an individual.

2.9 Release of information

Employees who under the regulations seek copies of or seek access to relevant manual or computer information on their named files must submit a written request for that information to the Data Protection Officer who is the Director of Corporate Services. The relevant information requested under the Data Protection Act, 1998, will be provided, if available, within forty days of receiving the valid request or an appointment made to view the relevant information depending on the format in which it is stored. An administrative charge of up to £10 maybe levied for copies of information. Employees will need to produce formal proof of their identification to gain access to named information.

The Personnel, Payroll and Superannuation Officers within the University receive various enquiries from external organisations regarding employees. These organisations can include:

- Pension Fund Institutions
- Bank/Building Societies
- Police Authorities
- Child Support Agency
- Tax Office
- Department of Social Security

The Human Resources and Payroll and Superannuation departments are obliged to provide information to the Police, Child Support Agency, Tax Office and Department of Social Security without gaining employee consent to release information. Information to banks/building societies will only be released with written consent from the employee. Heads of Schools should refer all such requests to the Human Resources or Payroll department.

Information requested concerning an employee will only be divulged in the following way:

a. Telephone enquiries

Telephone enquiries for personal information from institutions or companies will be refused.

Personal information will only be divulged with the written/verbal consent of the employee unless we are obliged to provide the information to organisations as detailed above.

The organisation requesting the information should provide written consent from the employee – if not then written/verbal consent will be sought by Human Resources or Payroll staff before divulging any information.

b. Written enquires

Written requests for information should be supported by written consent from the employee and be on official headed company paper as proof of legitimacy.

Again if no employee consent were given this would be sought by Human Resources or Payroll staff.

c. Transfer of information between departments

Occasionally there may be a need to transfer information/personnel files between departments if, for example, an employee transfers to another department.

Within the University data (name, department, staff number and start/end date) is passed to SUCS, Library, ID Card Studio, Staff Club and Occupational Health.

Any personal information requested will be, where possible, hand delivered to ensure confidentiality and security. If posted through the internal mail system this should be done so in envelopes marked '*PERSONNEL - IN CONFIDENCE*' in order to ensure confidentially is maintained at all times.

Human Resources and Payroll Services will follow the protocol described below in dealing with post:

- Addressed to named individual – this will be opened and put into the mail folder for that section/team
- Marked '*Confidential*' – it will be presumed that such post is official University business and in general it will be opened and put in mail folders.
- Marked '*Personnel - In Confidence*' – this is normally sensitive information for or about staff and will be passed through unopened to the addressee (or their private secretary).
- Marked '*Personal or Private*'– will be passed unopened to addressee.

2.10 Confidential waste

Human Resources, Payroll and department records contain confidential information on employees, therefore, procedures should be in place to ensure that information is disposed of correctly.

a. What is classified as confidential waste?

Confidential waste is regarded as any documentation that shows employee personal details, post details or salary details – any information which is personal and identifiable to an individual.

b. Where is confidential waste stored before being destroyed?

All confidential waste will be stored in secure areas accessible only to authorised personnel.

c. Who holds responsibility for disposal of confidential waste?

Within each department a designated individual should be responsible for the safe disposal of confidential waste at regular intervals.

2.11 Compliance with policy and responsibility

Any member of staff employed by the University of Southampton must ensure that they comply with this policy at all times. Failure to comply with any part of this policy could result in disciplinary action being taken up to and including dismissal.