University Guidelines on Employment Records

Introduction

The Data Protection Act 1998 replaces the Data Protection Act 1984 and it regulates the use of personal data.

The Act covers some manual records, such as those recorded on paper, as well as computerised records and is concerned with the processing of "personal data", that is, data relating to identifiable living individuals. Manual records covered by the Act include those held in filing systems arranged by name, or which contain information about individuals that can be found quickly and easily, e.g. indexed by name.

The Act grants employees the right to have a copy of the information that an organisation holds about them -and to correct any errors. Records must be held in a form that allows corrections to be made and there should be an audit trail recording corrections made.

What is an Employment Record

An employment record is a manual or electronic record which is capable of identifying an individual e.g by name or a reference number. It includes:

- Any record of which the contents relate exclusively to a named employee and which is held in the Human Resources Office

- Any record of which the contents relates exclusively to a named employee and which is held in the Salaries Office

- Any record of which the contents relate exclusively to a named employee and which is held in the School/Institute/Section.

What may an employment record contain

An employment record may contain any information required for the purposes of:

1. Statutory employment records, and or
2. Operational management and administration

It should not contain information that cannot legitimately to be shown to be related directly or indirectly to the employment of the employee concerned.

Managing Data Protection

The Director of Human Resources shall be responsible for ensuring that employment practices and procedures comply with the Act and for ensuring that they continue to do so.

Heads of School/Section and Line Managers should review what personal data they collect and remove any personal data, which is irrelevant or excessive.

The University Data Protection Officer (currently the University Archivist) is responsible for developing and implementing policies and procedures to engender a culture of compliance with the Act throughout the University.

Security

All employment records held within Schools/Sections should be held in secure cabinets and staff should only be able to gain access to employment records where they have a legitimate business reason to do so. Access should be restricted to named individuals designated by the Head of School/Section. There should be no shadow files or papers, other than "live" working documents relating to staff being processed by individual members of staff.

A system of recording who has accessed a personal record should be implemented.

Staff should also be aware of the potential risk in the transmission of personal data via fax or email. e.g. if recipient's fax machine is in a shared office.

Under no circumstances should personal records be taken off campus.

Sensitive Personal Data

The Data Protection Act defines "sensitive personal data " as personal data, which relates to an individuals :

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade Union membership
- Physical or mental health or condition
- Commission or alleged by him/her of any offence
- Proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

The University will ensure that explicit and informed consent of employees will be obtained for the processing of information which may include personal data. All sensitive data will be held within the Human Resources Office.

Sickness and Absence Records

All sickness and absence records will be held and collated within the Human Resources Office. Sickness and Absence Records will be made available to provide managers with information about those who work for them and to allow them address any problems that may arise.

Equal Opportunities Monitoring

Information about a worker's ethnic origin, disability or religion is sensitive personal data. As such this information will be held and collated within the Human Resources Office. Data will be made available to Schools/Section in an anonymised form.

Access to information

Employees will be allowed access to all files i.e. personnel record, payroll record and record held within school.

If an employee contacts you (a subject access request), you should notify the Human Resources Office as soon as possible. Any request to access information must be in writing and on receipt of such a request the Human Resources Office will respond within forty working days. A standard charge of £10 will be made. The Human Resources Office will maintain a record of all subject access requests.

If an employee has asked to access information which involves a third party permission should be sought from the third party regarding disclosure. If this is not possible account should be taken of the reasonableness of the release of such information and where possible the third parties identity should be removed.

References

Employees need to be aware of the difference between a reference given in a personal capacity and one given in a corporate capacity. A corporate reference is one given on behalf of the employer by one of its staff and the employer remains legally responsible for its contents. A personal reference is one given by a member of staff in an individual capacity and in data protection terms the employer is not liable for its contents. Anyone writing a personal reference should not use University headed notepaper.

Disclosure Requests

Any staff who receive requests for information regarding employees should pass the request to the Human Resources Office.

Discipline, Grievance and Dismissal

The Data Protection Act applies to personal data processed in relation to discipline, grievance and dismissal proceedings. The University's disciplinary procedures provide for warnings to expire. Any timespent warnings should be removed from the personal record or at the very least it should be disregarded.

Retention of Records

Past employee records will be held within archives for 20 years (currently under review).