**HR General Data Protection and Document Retention Policy**

DRAFT

# Context

This policy is written with due regard to the principles and guidelines laid out in the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR); UK Data Protection Bill (when enforced)[[1]](#endnote-1) (the “data protection legislation”) and other guidance available from relevant professional or regulatory bodies, such as the Information Commissioner. Data protection legislation controls how personal information is used by organisations, businesses or the government. Everyone responsible for using personal data has to follow strict rules called ‘data protection principles.’

This policy works in conjunction with the *University Records Management Policy* and the *Information Security Policy* and applies to personal data about individuals who can be identified from that data.

# Purpose

The purpose of this Policy is to ensure compliance with the data protection laws when processing (obtaining, holding, using, disclosing, disposing etc.) personal data by the HR Department.

Personal data is defined as:

‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’ (*GDPR Article 4(1))*

Personal data that reveals an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health, and individual’s sex life or sexual orientation is classed as “special categories of personal data” and merits specific additional protection.

This Policy applies to all personal data processed by the HR Department, regardless of whether that data is held on University equipment or personally owned equipment used inside or outside University premises.

In law the University is a “Controller” required to ensure that all personal data is processed in accordance with the data protection legislation. The Controller is also required to ensure anybody acting under their authority i.e. staff, students, contractors, who has access to the University’s personal data, only processes that data in accordance with the Controller’s instructions, which are:-

Personal data shall be:

* Processed lawfully and fairly and in a transparent manner in relation to the data subject;
* Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
* Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
* Accurate and, where necessary, kept up to date;
* Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
* Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures; and
* The Controller shall be responsible for and able to demonstrate compliance with these principles (*GDPR Article 5 Paras 1&2*)

**HR Staff responsibilities**

Access to personal data is only provided to authorised staff who need it to be able to perform their essential contracted duties.

Staff members processing personal data about employees, applicants or any other identifiable individual must comply with this policy. This includes any voluntary, short-term or contracted workers, consultants and agency personnel.

In particular staff members must ensure that they:

* Comply with the data protection principles when obtaining, using, disclosing or otherwise processing personal data.
* Keep all personal data securely in accordance with this Policy and the Acceptable Use Policy for IT Facilities and Equipment and related guidance;
* Only disclose personal data to persons authorised to receive it when it is appropriate to do so;
* Do not disclose personal data accidentally or otherwise, to any unauthorised person/third party (staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Director/Deputy Director of Human Resources. If neither are available queries should be directed to the University Secretary & Registrar);
* Maintain and dispose of personal data in accordance with the University’s Records Management Policy and HR retention schedules (as appended);
* Direct any queries regarding data protection, including subject access requests and complaints, to the University Secretary & Registrars’ Office;
* Report any data protection breaches to the University Secretary & Registrars’ Office in accordance with the *Personal Data Security Breaches Policy* and provide support to ensure the incident is appropriately investigated and resolved.
* Seek advice from the University Secretary & Registrars about data protection matters when in doubt

**Processors**

A “processor” is somebody other than University staff who processes personal data on behalf of the University – usually an external company working under contract.

When a processor is used, the University as Controller retains responsibility and liability for the secure and lawful processing of the personal data being processed. The Controller can only appoint a processor:

* who can provide sufficient guarantees about its technical and organisational security measures to protect personal data and meet the requirements of the GDPR;
* processes personal data only in accordance with the instructions of the Controller set out in a written contract;
* does not appoint a sub-contractor without the written permission of the Controller.

The *University’s Data Processor Procurement Guidance* should be followed when appointing a processor and advice sought from the University Secretary & Registrars’ Office when required.

**Retention Schedule**

|  |  |  |
| --- | --- | --- |
| **Type of Record** | **Retention Period** | **Legitimate Business/**  **Statutory/Legal Requirement** |
| Basic employee record: e.g. name, NI number, start date, end date, job title and reason for leaving | Permanently | Legitimate business need |
| Employee personal record (electronic and hard copy) including training and development, disciplinary and grievance, working time records, flexible working requests, types of leave (excluding sickness) | 6 years after employment ceases  (where parental leave has been taken, 18 years from the birth of that child) | References and potential litigation governed by Limitation Act 1980 |
| Recruitment files for unsuccessful candidates (including application, form, equality monitoring form, shortlisting and interview notes) | 6 months (dependent on complaint management/litigation). Details for successful candidates will be on personal files. | Equality Act 2010  UK Visa & Immigration (UK Border Agency Requirements)  Limitation Act |
| UKVI Right to Work Check documents (general) | Current guidance on gov.uk website recommends we should keep copies of right to work check documents for the duration of the person’s employment and for a minimum of two years after employment ceases – we will retain for 6 years after employment ceases | UK Visa & Immigration requirements  Limitation Act |
| UKVI Right to Work Check documents (Tier 2) | Current guidance on gov.uk website says that all right to work check documents must be kept for whichever is the shorter period of either:  • one year from the date you end your sponsorship of the migrant  OR  • if the migrant is no longer sponsored by you, the point at which a compliance officer has examined and approved these documents | UK Visa & Immigration requirements |
| Criminal records check (processed through GBG) | On line confirmation of clearance (not a certificate) retained as part of the personal file - retained for 6 years after employment ceases | Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 and those prescribed in the Police Act 1997 (Criminal Records) regulations, including the  Code of Practice in section 122(2)  Legitimate business need |
| Records documenting legal advice requested by, and provided to the institution concerning:  proposals for and/or the interpretation of legislation and advise in relation to employee relations/employment casework | 6 years after employment ceases | Legitimate business need  Limitation Act 1980 |
| Settlement Agreements (including Cot 3) | 20 years from date of agreement | Legitimate business need  Potential litigation governed by  Limitation Act 1980 |
| Redundancy details (including calculations of payments and notification to the Secretary of State | 6 years after employment ceases | Legitimate business need  Potential litigation governed by Limitation Act 1980 |
| Senior executives’ records (that is, those on a senior management team or their equivalents) | Permanently for historical purposes | Legitimate business need  CIPD recommendation |
| Salary and grading registers containing identifiable personal information | 6 years after employment ceases | Legitimate business need  Taxes Management Act  Limitation Act 1980 |
| ER casework registers containing identifiable personal information | 6 years after employment ceases | Legitimate business need  Limitation Act 1980 |
| Trade Union agreements | 10 years after ceasing to be effective | CIPD recommendation |
| JNCC and trade union related business | Permanently | CIPD recommendation (with respect to works Council business) |
| Employment and equality monitoring data relating to employee/s | 6 years after employment ceases | Legitimate business need  Employment/ER related legislation and activities  Equality Act |
| Accident books, accident records/reports | Statutory retention period: 3 years from the date of the last entry ( or if accident involves a child- until the age of 21) | Statutory authority: the Reporting of Injuries, Disease and Dangerous Occurrences Regulations 1995 (RIDDOR)(SI 1995/3163) as amended, and the Limitations Act 1980. See special rules governing hazardous substances. |
| Medical Records | Statutory retention period: 40 years from the date of the last entry | Statutory authority: The Control of Substances Hazardous to Health Regulations 1999 and 2002(COSHH) (Sis 1999/437 and 2002/2677) |
| Employee health records (eg. sickness absence dates/self certs/drs notes, or occ health referrals?) | 6 years after employment ceases | Management of Health and Safety at Work Regulations;  Contractual Claims for breach of employment contracts |
| Health records where reasons for termination of employment are connected with health, including stress related illness | 6 years after employment ceases | Limitation period for personal injury claim, reference and potential litigation by way of Limitation Act 1980 |

## Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Personal data | Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| Special categories of personal data | Personal data revealing the racial or ethnic origin of the data subject, or their political opinions, religious or philosophical beliefs, trade-union membership; genetic and biometric data, data concerning health, sex life or sexual orientation. |
| Processing | Any operation or set of operations which is performed on personal data or personal data sets, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, combination, restriction, erasure or destruction. |
| Controller | The natural or legal person, public authority, agency or other body which alone or jointly with others determines the purpose and means of processing personal data |
| Processor | A natural or legal person public authority, agency or other body which processes personal data on behalf of the controller. |
| Third party | A natural or legal person public authority, agency or body other than the data subject, controller, processor or persons who under the direct authority of the controller or processor are authorised to process personal data. |
| Personal data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise. |

1. [↑](#endnote-ref-1)