EDINBURGH NAPIER UNIVERSITY

STAFF PRIVACY NOTICE

Introduction

Edinburgh Napier University is a data controller for the purposes of the Data Protection Act 1998 (the Act) and processes the personal data of staff strictly in line with the Act and its notification to the UK Information Commissioner's Office (ICO). The Act requires the University to comply with the following eight principles to ensure that personal data is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with individuals' rights
7. Kept secure
8. Not transferred to other countries without adequate protection

Please note: As from 25 May 2018 the Data Protection Act 1998 will be replaced by the EU General Data Protection Regulation 2016.The University is currently preparing for the new legislation and will update this document on the 24 May 2018.

1. Rights under the Act

1.1 Your rights under the Act include to:

- Have access your personal data
- Object to data processing which causes damage and distress
- Prevent direct marketing & automated decision making; and
- Have your personal information corrected

1.2 You should contact Governance Services if you have any queries or concerns about the use or accuracy of your data or for information on how to exercise your rights under the Act.

2. Purposes for which Personal Data is obtained and processed by the University

2.1 Personal data is normally provided initially to the University by applicants and members of staff on a job application form and contract acceptance form. Examples of data held would include address, marital status, qualifications and supporting references. Information provided to the University in this context will be held securely in manual and electronic format for the purposes of the recruitment and selection process.

2.2 During the course of your employment further data will be added to and /or updated on the University's Human Resources database, HR Connect, by the

University and yourself through the Employee Self Service function. This will include your phone numbers, emergency contact details, bank details, pay slips, skills qualifications, diversity details, professional development and performance review processes and recording absences for the purposes of managing sickness absence.

2.3 All data held on HR Connect will be made available to staff in Human Resources (HR). Relevant restricted access, which will be actively audited by HR, will also be given to:

- Line Managers, through the People Manager function in order to carry out the full range of their line management responsibilities;
- Staff in Information Services for technical support purposes.
- Department for Learning and Teaching Enhancement for the purposes of managing and supporting the Teaching Fellowship Scheme and ENroute related courses

2.4 Where new requirements for access to HR Connect are identified, the requirement will be mapped out by the Director of Service/ Dean of School and approved by the Director of HR, prior to development in the system. This may include for example:

- Line Managers' PAs or other authorised nominee for support purposes with requests for leave and the input of sickness absence;
- School Support Managers for financial planning and budgetary purposes.

2.5 Relevant information will be transferred automatically from HR Connect to other databases including:

- Information Services for user registration for IT services;
- Information Services for emergency contact purposes
- The University card system, to enable a staff card to be issued to you;
- The Library system, to create your library access;
- The University's Data Warehousing database for management information reporting purposes
- Where applicable, to the SITS student records database to enable course tutors to be linked to students.

2.6 The University will process all personal and sensitive personal data strictly in accordance with the Act for statutory and legitimate administrative and business purposes, examples of which include:

- Managing HR processes e.g. salary and other payments, promotion, professional development and performance reviews, providing employment references
- Absence management including sickness absence recording, managing referrals to, and recommendations from, the external Occupational Health Service
- Mandatory reporting by Health & Safety of certain reportable accidents, dangerous occurrences and notifiable diseases
- Managing annual leave, flexi leave and other types of authorised leave or absence
- Monitoring compliance with the Equality Act 2010
- Handling grievance matters and disciplinary cases
- Preventing and detecting crime e.g. by use of CCTV and/or body worn radio

audio recordings

- Making external/statutory returns e.g. to the Higher Education Statistics Agency (HESA)
- Preparation of management information reports and statistics
- Mandatory reporting to HMRC
- Communicating with the Scottish Public Pensions Agency and the Lothian Pension Fund and Scottish Teachers Superannuation scheme for both contractual and auto-enrolment purposes, including the auto-enrolment of eligible jobholders and the management of opt-ins/opt-outs to the scheme
- Assessing each member of the University's workforce to identify into which category of worker they fall, for auto-enrolment into a workplace pension scheme
- Maintaining contact with former employees

2.7 Staff should be aware that for operational and business reasons, senior managers may give their PAs, Executive Support Assistants or other key support staff member access to their Outlook folders, calendars and/or mailbox.

2.8 On termination of your employment, appropriate records will be retained in accordance with the HR Records' Retention Schedule. The remainder will be securely destroyed in accordance with the University's guidance on Records Disposal and the Use of Consoles.

3. Processing Sensitive Personal Data

3.1 The Data Protection Act 1998 defines certain personal data as "sensitive personal data". This includes ethnicity, physical or mental health and criminal convictions. The University holds such data for e.g. equal opportunities monitoring, mandatory reporting to the Health and Safety Executive, the provision of occupational health services to individuals and to meet its obligations to make reasonable adjustments under the Equality Act 2010.

3.2 If a member of staff states at any time during their employment that they consider themselves to have a disability, this information will be shared on a strictly need to know basis to ensure that reasonable adjustments are made for them to carry out the duties of their post.

3.3 The University is required to obtain information about past criminal convictions as a condition of employment for certain posts. Disclosure Scotland checks are undertaken in respect of staff who work with young and/or vulnerable persons.

3.4 Information on a member of staff's health may be required as a condition of employment. The University may also in exceptional circumstances contact third parties e.g. medical professionals or next of kin, concerning the health of a member of staff when it is considered reasonable and/or in the best interests of the member of staff to do so. The University will attempt to gain the prior consent from the member of staff but where consent cannot or will not be given, it may act without consent. The Director of HR or nominated direct report in HR, must be consulted before any contact is made with third parties.

3.5 Sensitive personal data may also be shared for the purposes of monitoring absence, as permitted under the Act and in accordance with the University's Sickness Absence Policy.

4. Publishing Personal Data

4.1 Registration with Information Services will result in a member of staff's name, photo, department/section, job title, email address, room and telephone numbers being listed in the University's Staff Directory on the staff intranet. Staff may opt out of their photo being used for this purpose.

4.2 A version of the Staff Directory, searchable by name and job title, is made available on the University's website.

4.3 Academic members of staff have the facility to have additional information such as their academic qualifications, brief biography, professional/research interests, activities and outputs published on the University's external website as required for business/academic purposes. This will follow a standard template format, with information being uploaded to the website from the Research Management System, where staff can input/upload their own details and are therefore responsible for ensuring the information is current and correct at all times.

4.4 Departments may publish details of support staff's duties and responsibilities in relation to their roles elsewhere online.

4.5 In exceptional circumstances, and in consultation with her/his line manager, a request by a member of staff to have their details removed from the University's Staff Directory in part or in full, must be referred to the Director of HR, who will consult with the relevant Dean of School, Director of Service and Governance Services, as necessary, for a decision to be made.

5. Use of Images

5.1 Each member of staff is required to provide their digital image to HR for the issue of their University staff card. This card should be carried with them at all times and will be used for the purposes of identification, using University facilities and gaining access to certain areas of the University.

5.2 The University may commission photography or film at any of its campuses, for specific events e.g. the award ceremonies or for use in its promotional materials. The seeking of any necessary consent will be in accordance with the University's guidance on Photography and Film in the Data Protection Code of Practice.

5.3 The use of images in the University's Staff Directory is referred to in 4.1 above.

6. External Study, Employment and Placements

6.1 Where a member of staff's employment with the University requires study, employment or a placement at another organisation it will be necessary for the University to transfer personal data to the external university or employer, whether this is within the UK or abroad. This will be done in accordance with the Act and any appropriate University guidance.

6.2 Staff should be aware that some countries outwith the European Economic Area (EEA) have lower standards than the EEA for the protection of personal data.

7. Information Services

7.1 The University routinely logs information about use of IT facilities for statistical purposes and to ensure effective systems operations.

7.2 The University may also monitor electronic communications in accordance with the Monitoring and Logging Policy and the University's Information Security Policies, specifically for the purposes of preventing or detecting crime.

7.3 Where a member of staff has left the University or is absent from the University for any reason including long term sickness, and contrary to University policy, has retained records on network areas which only they can access (e.g. 'H' or 'C' drives, OneDrive, mySite, staff email account or on their desktop) which are necessary for business continuity, the investigation of complaint or disciplinary matters or other legitimate business reasons, a request for access to such records may be made to the Director, Information Services. The Director will consult with the relevant member of the University's Leadership Team in considering the request and if granted, authorised Information Services staff will oversee access to these records to ensure this is strictly limited to the minimum required to retrieve and/or provide such records.

7.4 The University complies with the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA) in all such monitoring activities. Requests for personal data in monitoring logs will be considered by the Director of Information Services who will consult with the relevant member of the University's Leadership Team and decide whether the request is to be granted and if so, the minimum data to be disclosed in order to achieve the purpose.

8. CCTV and Body Worn Radio audio recordings

8.1 The University's premises and grounds are monitored by CCTV systems for the purposes of public safety and security and the prevention and detection of crime. CCTV footage may also be used for investigations or proceedings arising under the University's Complaints Handling or Staff Disciplinary Procedures.

8.2 In the event of a serious incident arising and strictly in accordance with University procedures and guidance, the University's Security Officers may make body worn radio audio recordings, which may be used in criminal investigations or investigations or proceedings arising under the University's Complaints Handling or Staff Disciplinary Procedures.

9. Use of Personal Data in Research

9.1 Staff personal data (but not sensitive personal data) may be processed on an anonymous basis for academic research purposes, where there is benefit either to the researcher alone or the researcher and University combined, on the basis that the results of the research will not lead to decision-making about an individual or groups of individuals.

9.2 Where a researcher proposes to use sensitive personal data, e.g. ethnicity or health, this will be discussed with the Director of HR or nominated direct report in the first instance and explicit consent will be sought from the individual members

of staff concerned before any data is disclosed.

10. Disclosures to Third Parties

10.1 Agents & Advisers

The University may need to disclose the personal data of members of staff to organisations contracted to work on its behalf, which may include its pension providers, insurers or legal advisers.

10.2 Auditors, Alumni & Researchers

The University may also disclose data to auditors undertaking audits and investigations, selected individuals acting on behalf of the University e.g. alumni organising alumni events, external organisations undertaking market research or academic researchers, provided that no personal data is published.

10.3 External Research funders

In accordance with requirements of University research projects for which external funding has been granted, the data of relevant staff involved at any stage of such a project may be disclosed where: there is a legitimate interest to do so, it is a condition of funding or is otherwise necessary for the performance of a relevant research contract. Disclosures will be made strictly in accordance with the University's Data Protection Code of Practice and may include e.g. redacted copies of employment contracts and payslips or personal financial data extracted from HR Connect by authorised HR staff. Further information is available on the Research and Innovation Office (RIO) website.

10.4 Police and other third parties

In response to a formal written request and after consultation with the Director of HR or nominated direct report or Governance Services, personal data may be disclosed to the Police and other external third parties as permitted under the Act, where it is required:

- to apprehend or prosecute an offender or prevent or detect a crime
- for the purposes of the assessment or collection of any tax or duty

10.5 Mandatory reporting to the Home Office UK Visa and Immigration Agency

Under the Points Based Immigration System, the University is a highly trusted licensed sponsor for staff recruited from outside the European Economic Area (EEA) and Switzerland and as such must comply with certain reporting requirements to the Home Office.

10.6 Requests under the Freedom of Information (Scotland) Act 2002 (FOISA)

The University is subject to FOISA and routinely receives requests about University business which may include information that identifies individual staff members. The University is only obliged to provide information about staff in their professional capacity and will not disclose data held in relation to them as a private individual if this would breach the Data Protection Act 1998 (DPA). However the University must then go on to consider the public interest test i.e. whether the interests and rights of the public under FOISA outweigh those of the individual's right to privacy under the DPA. If in exceptional circumstances that was considered to be the case, then the University would be expected to release

the information.

10.7 Debt Collection Agencies

In certain circumstances the University will pass the personal data of staff debtors to an external debt collection agency if the University has been unable to recover the debt by normal internal, financial or HR processes.

10.8 Scottish Funding Council

The University has a statutory requirement to disclose staff personal data to the Scottish Funding Council (SFC) and/or its nominees/successors. The University may also disclose personal data to SFC and its partner bodies for the purposes of the Research Excellence Framework.

10.9 Her Majesty Revenue & Customs (HMRC)

The University is required to report PAYE information to HMRC in real time i.e. Real Time Information (RTI). HR will send details to HMRC every time an employee is paid, at the time they are paid and send this information through HMRC's secure gateway as part of their routine payroll process.
The information provided will be:

- Name
- Date of birth
- National Insurance Number (NI)
- Gender
- Home address – if the NI number is not available then this must be given

11. Disclosures to HESA

11.1 The HESA Staff Record

We are required annually to send some of the information we hold about you to the Higher Education Statistics Agency (HESA). This forms your HESA Staff Record which does not contain your name or contact details. Please read the full text of the HESA Staff Collection Notice which explains how your personal data will be used.

12. FURTHER INFORMATION

Internal sources

- The University's Data Protection Code of Practice
- Contact Governance Services
  dataprotection@napier.ac.uk;
- The University's Equality and Diversity website

External sources

- Lothian Pension Fund Pensionweb privacy statement
- Lothian Pension Fund FOI and data protection statement
- STSS data protection statement and STSS privacy statement
- Points Based Immigration System: Tier 2
  www.ukba.homeoffice.gov.uk/workingintheuk/tier2/general/
- The UK Information Commissioner

Document Control Information	
Title	Staff Processing Statement
Version	v.1.08
Author	Governance Services
Date Approved	By University Information Governance Group 20160916 By Digital Strategy Investment Committee 20160927 Minor update Governance Services 20170809 Minor update Governance Services 20171201
Review Date	Biennially or earlier as appropriate
Scope	All University employees.