EDINBURGH NAPIER UNIVERSITY

STAFF PRIVACY NOTICE

Introduction

Edinburgh Napier University is a data controller for the purposes of UK Data Protection legislation ("the legislation"), that is, the UK Data Protection Act 2018 ("DPA 2018") and the General Data Protection Regulation: EU 2016-679 ("GDPR") as amended by "EU Exit" Regulations 2019, now known as the UK GDPR, and processes the personal data of staff in compliance with the legislation and its notification to the UK Information Commissioner's Office (ICO). The University is committed to compliance with the legislation and protecting staff member's personal data.

1. Categories of Personal Data Processed

The University processes personal data for the purposes set out in this notice and this may include: personal and family details; lifestyle and social circumstances; education, employment and professional membership details, or similar, relevant to your role; financial details; disciplinary and attendance records; details of complaints, incidents and grievances; goods or services provided; visual images, personal appearance and audio recordings; information used to publish university promotional material; responses to surveys and online identifiers.

We also process sensitive or special categories of personal data that may include: racial or ethnic origin; trade union membership; religious or other similar beliefs; physical or mental health details; sexual life or sexual orientation; biometric data; criminal proceedings, outcomes, sentences and PVG Scheme data.

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.

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, contact details, emergency contact details, bank details, pay slips, skills qualifications, diversity details, performance, personal development, continuous professional development 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 is managed and audited by HR, will also be given to:

- Line Managers and their 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;
- PA's may have delegated responsibility to act on behalf of Senior Managers which includes access to HRConnect for limited purposes e.g. sickness absence input.

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 People and Services, prior to development in the system. These are assessed on the role/service and delegated responsibility requirements.

2.5 Relevant information will be transferred automatically between HR Connect and other databases including:

- Information Services, and externally provided systems such as Microsoft, for user registration for IT services and the ongoing provision of relevant software systems to enable employees to undertake their contracted duties.
- Information Services and relevant software services for emergency contact purposes, staff card production and to enable IS to confirm your identity.
- 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, e.g. to enable course tutors to be linked to students.
- The Worktribe system for research management purposes.
- Finance for purposes of informing the budgeting process.
- Where third parties or third party software is used relevant information will be provided e.g. the administration of the staff communications/survey system, Poppulo.
- Moodle and eSkillz to record and manage key learning event completion.
- The University primarily uses Microsoft as our service provider, which acts as a data processor, handling and processing your personal data in accordance with contractual safeguards, our privacy policies and applicable data protection legislation. The University also uses many other software products to provide the necessary tools and functionality to enable it to operate and undertake its functions, as set out in its Statutory Instruments. Additionally, these systems may use system generated data to provide services, for diagnostic, product improvement and troubleshooting purposes, etc.

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

- Managing HR processes e.g. salary and other payments, promotion, performance, personal and career development, providing employment references, etc. This may also include processing professional membership information, where relevant to your employment, including accessing information available from public sources. Where professional membership is a role requirement or staff are part of a corporate membership, the University may share personal data with those parties e.g. current membership, disciplinary matters, fitness to practice, etc. as relevant and required by those bodies.
- 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 Legislation 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), UCEA, Athena Swan, REF, etc.
- Seeking advice from UK Government bodies on research activities to ensure compliance with Export Controls and National Security Legislation
- Preparation of management information reports and statistics.
- Mandatory reporting to HMRC.
- Communicating with the Scottish Public Pensions Agency, 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 Staff are required to complete register of interests declarations and returns as determined by ULT. Please see the Conflicts of Interests Policy Framework.

3. Processing Special Categories (Sensitive) Personal Data

3.1 The legislation defines certain personal data as "special category" (sensitive personal data). This includes ethnicity, physical or mental health and criminal convictions. The University holds such data for a number of reasons including equal opportunities monitoring, mandatory reporting to the Health and Safety Executive, fitness to work assessments, the provision of occupational health services to individuals, undertaking Health Surveillance checks for employees in relevant roles, etc., to meet its obligations to make reasonable adjustments under the Equality Legislation 2010, Health & Safety legislation, etc.

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 to enable them to carry out the duties of their post. Employees are encouraged to update their own HRConnect record and ensure Disability Reasonable Adjustment Agreement is completed. See the Attendance Management Policy and Disability guidance for more information.

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 process this data as allowed under the legislation without consent (Article 9 (2)(b) & (h)) where processing is necessary for the purposes of preventative or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, etc.. The Director of People and Services 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 Legislation and in accordance with the University's Attendance Management 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 People and Services, 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. Staff are encouraged to carry this with them at all times on University premises, as it may be required for security and access purposes.

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 Legislation and any appropriate University guidance.

6.2 Staff should be aware that some countries outwith the UK, European Economic Area (EEA) and other 'adequate' countries, have lower standards than the UK Data Protection legislation for the protection of personal data, however. University staff entering into contracts with external organisations are obliged to ensure that the appropriate safeguards and contracts/agreements are in place to ensure adequate measures are in place to protect personal data.

7. Information Services

7.1 User data is recorded by all ICT systems. The University routinely logs information about use of IT facilities for network security, statistical purposes and to ensure effective systems operations. This includes IP addresses as automatically logged by systems.

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 unlawful acts and dishonesty, etc.

7.3 Where members of staff have retained records on network areas which only they can access (e.g. 'H' or 'C' drives, OneDrive, 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, the University reserves the right to access these records and areas of the University network.

7.4 The University complies with data protection legislation and the Regulation of Investigatory Powers Legislation 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.

7.5 The University may conduct searches for information as required by other legislation e.g. the Data Protection Act 2018 in order to action Data Subject rights requests.

7.6 Information Services require access to limited personal data specifically for the purposes of authenticating the identity of users asking for assistance.

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, Staff Disciplinary Procedures or Student Conduct Regulations.

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 Staff personal data will be used, as appropriate, for the purposes of course evaluation.

9.3 Where a researcher proposes to use sensitive personal data, e.g. ethnicity or health, this will be discussed with the Director of People and Services 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 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 redacted copies of employment contracts and payslips or personal financial data extracted from HR Connect by authorised HR staff, etc. The University adheres to the terms of the Safeguarding Research Framework which may also require data sharing with relevant external parties. Further information is available on the Research Innovation & Enterprise (RIE) intranet pages.

10.4 Police and other third parties

Disclosures may be made to the Police and other regulatory bodies and third parties where it is exempt under Schedule 2 of the Data Protection Act 2018 e.g. for the purposes of public safety, security, the prevention and detection of crime and fraud, and the assessment or collection of any tax or duty, etc.

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) Legislation 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 legislation. 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. 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.

10.10 Other Statutory Bodies

- The UK Information Commissioner's Office – in the event they are required to investigate an appeal or other investigation.
- The Scottish Public Services Ombudsman – in the event of an investigation into a complaint.

10.11 References

Where a staff member has been the subject of disciplinary proceedings for a matter of serious misconduct and a finding made, this and any action taken may be referred to in a reference. More serious criminal issues might, in relation to the Rehabilitation of Offenders Act, be treated as 'spent' five years after the occurrence unless the context (e.g., working with children or professional standards) requires disclosure or if it is in relation to a regulated role as defined by Disclosure Scotland and subject to a PVG membership.

10.12 Collaborating and Business Partner Organisations

The University will share staff personal data, as necessary, with third party organisations with which it has a contractual relationship for business purposes to enable the contracted services to be provided.

10.13 External Systems and Services Providers

The University will share staff personal data with systems and services providers where required and necessary to provide such systems and services to employees e.g. external training providers for the purposes of training provision and completion reporting (eSkillz, Meta Compliance, Emerald, etc.), pension and benefits providers (AVC-Wise, etc.), to send communications in emergency situations (SafeZone), travel risk assessment provider (Garda World), Staff ID Card provider, etc.

10.14 UK Government Bodies for assessment of National Security risks in Research and Innovation activities

The University will share information about research projects as part of the due diligence processes where it is identified that the research may be in scope of the Export Controls or National Security and Investment legislation. This may involve sharing the full applications forms including details of all people identified as working on the project (whether based at Edinburgh Napier or elsewhere) to advisors at BEIS for assessment. If the assessment determines we need to report officially or apply for a licence for the activity, we will share all information required to the appropriate bodies to ensure compliance with the legislation.

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. Please read the full text of the HESA Staff Collection Notice which explains how your personal data will be used.

12. Legal Bases for Processing

12.1 The majority of the processing of staff personal data will be for the purposes of maintaining and administering employee contracts and the contractual relationship. The legal basis relied on will be Article 6(1)(b): "processing is necessary for the performance of a contract

to which the data subject [employee] is party". This includes services that are provided as part of employee benefits e.g. library services.

Others include:

12.2 Article 6(1)(c): "processing is necessary for compliance with a legal obligation to which the controller is subject", e.g. statutory returns to HESA, HMRC, SFC, UK Visa and Immigration Agency, FOI(S)A, DPA, etc.

12.3 Article 6(1)(d): "Processing is necessary in order to protect the vital interests of the data subject or of another person", e.g. in emergency situations (Article 9(2)(c) applies for special categories of personal data).

12.4 Article 6(1)(e):"Processing is necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller", namely the University's Statutory Instruments: "for the objects of providing education, carrying out research, and promoting teaching, research and general scholarship" and the administration thereof, e.g. certain aspects of managing and supporting the Teaching Fellowship Scheme and ENroute related courses, promoting teaching, research and general scholarship, promotion of the University and its staff.

12.5 Article 6(1)(f): "Processing is necessary for the purposes of the legitimate interests pursued by the controller, where this is outside of the University's official authority, e.g. monitoring ICT services for the legitimate interest of ensuring acceptable use policies and legislation are complied with.

12.6 Article 6(1)(a): "Where consent for the processing has been given" e.g. points 5.2 and 9.2.

12.7 Article 9(2)(b): Processing is necessary for the University to exercise its obligations under employment, social security and social protection laws e.g. HMRC, and DPA 2018 Schedule 1 Part 1 (1) Employment, etc. purposes.

12.8 Article 9(2)(f): "Processing is necessary for the establishment, exercise or defence of legal claims", e.g. where tribunal or legal action is involved.

12.9 Article 9(2)(g): "Processing is necessary for reasons of substantial public interest" as allowed for in the derogations in the DPA 2018 Schedule 1 Part 2, including, but not limited to:

- S.8 Equality of opportunity or treatment
- S.9 Racial and ethnic diversity at senior levels of organisations
- S.10 Preventing or detecting unlawful acts
- S.11 Protecting the public against dishonesty
- S.12 Regulatory requirements relating to unlawful acts and dishonesty, etc.
- S.14 Preventing fraud
- S.16 Support for individuals with a particular disability or medical condition
- S.17 Counselling, etc.
- S.18 Safeguarding of children and individuals at risk
- S.19 Insurance
- S.21 Occupational pensions

12.9 Article 9(2)(h): "Processing is necessary for the purposes of preventative or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, etc.", e.g. points 2.6 and 3.4.

Additionally:

12.10 The legislation allows for archiving in the public interest, scientific or historical purposes or statistical purposes where appropriate safeguards are in place and it is not incompatible with the original purposes for processing e.g. statistical analysis for operational reports and returns, maintenance of the University archive records and research where consent is not required.

13. Rights under the Legislation

13.1 Your rights under the Legislation include to:

- Have access to your personal data
- Apply for rectification where your data is incorrect

- Take steps to prevent processing which may cause you harm or distress
- The right to withdraw consent where this is the legal basis for processing.

Subject to conditions relating to the purpose of processing, additional rights include:

- Erasure of certain personal data
- Restriction of processing
- Receive a copy of the personal data provided by yourself in a machine readable format
- Object to processing in certain circumstances
- Not to be subject to automated decision making, including profiling.

For more information about your rights please visit: staff.napier.ac.uk/accessyourinfo.

14. Security and Retention of your Personal Data

14.1 For services provided locally by Information Services, information is stored on servers located in secure University datacentres. These datacentres are resilient and feature access controls, environmental monitoring, backup power supplies and redundant hardware. Information on these servers is backed up regularly. The University has various data protection and information security policies and procedures to ensure that appropriate organisational and technical measures are in place to protect the privacy or your personal data – for more information please click here.

14.2 Records containing personal data are kept in accordance with the University's records' retention schedules.

16. Other

16.1 The University does not undertake any automated decision-making processes.

16.2 It is important that the data the University holds about you is accurate and current. It is employees' responsibility to keep their personal details up to date and inform us of any changes that may be necessary during the employment relationship with the University. This can be done using HRConnect or by contacting the Human Resources team.

16.3 The University uses social media tools for various communications - these are 'opt in' services and by registering to use them you must agree to the social media site's Privacy Policy and Terms & Conditions. You must also comply with the University's Social Media Usage Policy.

16. Further Information

The University reserves the right to update this Staff Privacy Policy at any time and will remind employees to review it regularly. We may also notify you in other ways about the processing of your personal data.

Additional information is provided in the University's 'layered' Privacy Notices. You can access all the University's privacy notices using the following link: https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/statement.aspx

You have a number of rights available to you with regards to what personal data of yours is held by the University and how it is processed – to find out more about your rights, how to make a request and who to contact if you have any further queries about Data Protection please see the information online using the following URL: https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/default.aspx

Internal sources

- The University's Data Protection Code of Practice
- Contact Governance Services, email 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.3.2
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 Update Governance Services 20170326 for UIGG approval 20180328 Update HR and Governance Services 20190612 for UIGG approval 20190613 Updated by Governance Services 20220314. RRC Convenor approval 20220314 Updated by HR and Governance Services 20220421 for UIGG and RRC Convenor approval 20220623 Updated by RIE for UIGG and RRC Convenor approval 20221002 Minor update Governance Services for RRC Convenor approval 20250106
Review Date	Biennially or earlier as appropriate
Scope	All University employees.