Edinburgh Napier UNIVERSITY

DATA PROTECTION POLICY STATEMENT
and
APPROPRIATE POLICY DOCUMENT FOR SPECIAL CATEGORY AND CRIMINAL CONVICTION PERSONAL DATA PROCESSING

PART 1: DATA PROTECTION POLICY STATEMENT

Edinburgh Napier University ("the University") is committed to protecting the rights and freedoms of individuals with respect to the processing of their personal data. This is done in accordance with:

- Data Protection legislation ("the legislation"), now known as the UK GDPR. The Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 amended the EU General Data Protection Regulation 2016 (EU GDPR) and together with the Data Protection Act 2018 the legislation is now known as the "UK GDPR" and referred to as "the legislation" below.
- Associated legislation, in light of relevant case law and appropriate guidance (e.g. from the ICO)
- The University's registration with the UK Information Commissioner.

1. COMPLIANCE

1.1. All individuals (employees, students, agents, associates, contracted parties both paid and unpaid, etc.) processing personal data on behalf of the University are required to comply with:

- Data protection law
- The University's Data Protection Code of Practice, Information Security and Manual Data Security Policies
- Associated University policies, procedures and guidance on the provisions and practical implementation of the legislation

1.2. These requirements apply to all personal data created and received, regardless of where it is held and irrespective of the ownership of the equipment used, if the processing is for the University's purposes.

1.3. Any breach of the University's policies, procedures or guidance may result in liability for the University and internal disciplinary action being taken.

2. RESPONSIBILITIES

2.1 All employees and agents processing personal data for and on behalf of the University are responsible for ensuring that any such processing complies with the legislation.

2.2 All line managers are responsible for ensuring that the processing of personal data carried out in their School/Service Area is compliant with the legislation and that employees reporting to them are aware of their responsibilities under the legislation and have received training.

2.3 Governance Services and the Data Protection Officer (DPO) are responsible for overseeing compliance, developing guidance and providing advice and training to employees.

2.4 The University Secretary has overall responsibility for ensuring that the University complies with data protection and associated legislation

3. THE DATA PROTECTION PRINCIPLES

The Data Protection legislation sets out six principles governing the use of personal information with which all University users must comply unless an exemption applies. These principles ensure that personal information is:

1) Processed fairly, lawfully and transparently
2) Processed for limited purposes
3) Adequate, relevant and limited to what is required only (data minimisation)
4) Accurate and up to date
5) Not kept for longer than is necessary for the purposes it was collected and processed for (storage limitation)
6) Kept securely using both technical and organisational measures (integrity and confidentiality)

Additionally, there are requirements to:

7) Keep written records of processing to demonstrate compliance (accountability)
8) Process personal in line with individuals' rights
9) Not transfer personal data to other countries without adequate protection

The University's Data Protection Code of Practice provides further information and is available at: Data Protection Code of Practice

PART 2: SPECIAL CATEGORY (SENSITIVE) AND CRIMINAL CONVICTION PERSONAL DATA PROCESSING

The University processes special category data, as defined in Article 9 of the UK General Data Protection Regulation (GDPR). We also process some criminal offence data, as defined in Article 10 of the General Data Protection Regulation (GDPR) and section 11(2) of the Data Protection Act 2018 (DPA 2018). This data must be processed in accordance with the requirements of the GDPR and, where applicable, Schedule 1 of the Data Protection Act 2018 (DPA 2018).

Some of the conditions for processing special category and criminal offence data, as set out in DPA 2018 Schedule 1, require us to have an Appropriate Policy Document (APD) in place. The APD must set out and explain our procedures for securing compliance with the principles in Article 5 of the GDPR and our policies regarding the retention and erasure of such personal data.

1. PURPOSE

1.1 This document explains our processing in relation to special category and criminal offence data and satisfies the requirement to have an APD in place, as set out in Schedule 1, Part 4 of the DPA 2018.

2. SCOPE

2.1 This policy applies to all processing of special category or criminal offence data, undertaken by or on behalf of the University, which is based on a condition in Schedule 1 of the DPA which requires an APD.

2.2 Special category data is defined at Article 9 of the GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

2.3 'Criminal conviction data' covers processing in relation to criminal convictions and offences or related security measures. It also includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing.

3. CONDITIONS FOR PROCESSING

3.1 We process special categories of personal data as set out in the University's Privacy Notices, available online.

4. COMPLIANCE WITH THE PRINCIPLES

4.1 Principle (a): lawfulness, fairness and transparency

We have put in place appropriate measures to ensure we meet this principle. These include:

- ensuring that we always meet relevant lawful basis/bases for processing, including at least one of the conditions in Schedule 1, where required;
- providing clear and transparent information about why we process personal data including our lawful basis for processing in the University Privacy Notices and
- setting out our main processing activities in the University Privacy Notices;

4.2 Principle (b): purpose limitation

Our purposes for processing are set out in the University Privacy Notices.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

4.3 Principle (c): data minimisation

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

4.4 Principle (d): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

4.5 Principle (e): storage limitation

All special category or criminal conviction data processed by us is retained for the periods set out in the University Records Retention Schedules. Retention periods for this data are based on our business needs, best practice and/or legal obligations. Our retention schedules are reviewed regularly and updated when necessary.

4.6 Principle (f): integrity and confidentiality (security)

Electronic information is processed within our secure network. For services provided locally by Information Services, information is stored on servers located in secure University data centres. These data centres 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. The University makes use of a number of third party, including "cloud", services for information storage and processing. Through procurement and contract management procedures the University ensures that these services have appropriate organisational and technical measures to comply with data protection legislation. Specific local processes include secured paper forms and files, password protected e-files, encrypted emails, etc. and the use of third party systems which the University ensures have the necessary technical and organisational security and contractual measures in place to protect the data.

Hard copy information is processed in line with appropriate security procedures. Both our electronic systems and physical storage have appropriate access controls applied.

The systems we use to process personal data allow us to erase or update personal data at any point in time, where required.

4.7 Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- the appointment of a Data Protection Officer who has a direct reporting line to the University Secretary;
- taking a 'data protection by design and default' approach to our activities;
- maintaining documentation of our processing activities;
- adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors;
- implementing appropriate security measures in relation to the personal data we process; and
- carrying out data protection impact assessments for our high risk processing and where otherwise deemed helpful.

We regularly review our accountability measures and update or amend them where required.

5. RETENTION

5.1 The University's Record Retention Schedules are available online internally using the following link: Records Retention Schedules

CONTACT

Queries about this Policy can be directed to:
Governance Services - dataprotection@napier.ac.uk

Document Control Information	
Title	Data Protection Policy Statement
Version	V4.0
Author	Governance Services
Date Approved	Reviewed and approved (V1.1): 2009 by RRAM and PEG Second review and approval: (V2.0) 24/05/17 Convener of DSIC Third review and approval: (V2.1) 29/10/19 by UIGG and the Convenor of RRC Fourth review and approval: (V3.0) 27/10/21 by UIGG and the Convenor of RRC Fifth review and approval: (V4.0) 23/06/22 by UIGG and the Convenor of RRC
Review Date	Biennially
Scope	All individuals processing personal data on behalf of the University