Layered Privacy Notice

Activity/Processing being undertaken: Staff Recruitment

Edinburgh Napier University as the "Data Controller" is providing you with this information in order for us to comply with UK Data Protection legislation (Data Protection Act 2018 (DPA 2018) and UK-GDPR), which requires us to tell you what we do with your personal information.

Below we have outlined how we manage your data for the purposes of recruitment, specifically managing data received from applicants at application stage and as potential new employees.

Why are we collecting your information/what we are doing with it (purposes)?

All new applicants submitting job applications to Edinburgh Napier University are required to provide personal data as part of their application in order for the University to:

- assess and administer your application for employment
- communicate with you in relation to your application
- comply with any legal or regulatory obligations, including compliance with the Equalities Act 2010
- to facilitate or advise you of other employment opportunities that may interest you
- reporting and statistical analysis
- further processing will take place in respect of successful applicants, as follows:

Specific aspects of application assessment and administration are dealt with by external contractors, more detail is provided below:

- pre-employment screening
  Applicants will be subject to pre-employment screening and will submit their own details to our chosen vetting agency. Please note that this is changing from Core Asset Verify to Capita PLC Security Watchdog in February 2022. Our standard checks for all roles within the University will be identified, and employment verification checks relevant to the role undertaken by the University's external provider. The purpose of performing these checks is to ensure fairness and transparency of the process for all stakeholders, ensure that the University complies with other legal requirements on it, and ultimately to verify your personal data and application details. The University will receive a report from our external pre-employment screening agency after checks have been made and before the position is awarded to the successful candidate.
- health assessment
  Applicants are required to complete an online health questionnaire – this exercise is administered by the University's Occupational Health (OH) provider, Optima Health. The questionnaire will collect personal data including health data.

In addition, information will be gathered at the appropriate stage in the recruitment process e.g. successful applicants, to check eligibility to work in the United Kingdom, in line with UK legislation.

Who has access to your personal data?

Applicants' personal data will be shared internally with HR employees and relevant managers in the School/Service Area involved in the specific recruitment & selection process e.g., hiring managers, interview panel members, etc. Appropriate access controls are in place.

We share your data with the following third parties:

- Capita PLC Security Watchdog. You can review their privacy policy here: Privacy Policy - Security Watchdog, part of Capita plc
- MCL Medics, our Occupational Health provider. You can review their privacy policy here.
- We also use DocuSign, a third-party software, for processing the personal data of successful candidates for the purposes of collecting your electronic signature on your contract of employment and for the on-boarding process. You can review their privacy policy here.
- Disclosure Scotland to obtain criminal record checks, to assess suitability to perform specific roles i.e., regulated roles which require PVG and roles assessed as requiring a disclosure check.
- Yoti – UK Digital Identity and Attributes Trust Framework – IDV, who can support the University with right to work in the UK checks. You can review their privacy note here.

The University undertakes to maintain your information securely and will restrict access to employees, our professional advisers, authorised agents and contractors on a strictly need to know basis. We will only disclose your data to external third parties (other than any specified above) where we:

- Are required to do so under a statutory or legal obligation, or
- Are permitted to do so by Data Protection legislation.

What is the legal basis for processing?

- Article 6(1)(b): Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, in this case applying for employment with the University.
- Article 6(1)(c) : Processing is necessary for a legal or statutory obligation
- Article 9(2)(b) and DPA 2018 Schedule 1 Part 1: Processing special category personal data is necessary for the University to exercise its obligations under:
    - 1. employment laws, that is, for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment
    - 2. health care purposes, that is, the assessment of the working capacity of an employee, preventative or occupational medicine, etc.
- 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:
    - 8. equality of opportunity or treatment

- 11. protecting the public against dishonesty in the exercise of a protective function e.g. safeguarding
- 12. regulatory requirements relating to unlawful acts and dishonesty, etc.
- 16. support for individuals with a particular disability or medical condition
- 18. safeguarding children and individuals at risk

How are we collecting this information?

Edinburgh Napier University will ask you to complete a secure online application form and if successful you will then provide further information to our third-party suppliers, in order for them to complete their vetting and health checks.

What information are we collecting (whose information and what type of personal data)?

- Applicants and potential employees.
- Capita plc Security Watchdog will collect a copy of your identification, any relevant visa/right to work information, personal email address, phone number/other contact details as necessary, education certificate/s, previous employment details, references and in some cases they may required to process your financial information e.g. your bank statements and other information to undertake pre-employment verification and criminal conviction checks* (please see below). They may also conduct P.V.G. and B.P.S.S. checks, which may be required for specific roles. Only checks appropriate to the position being applied for will be undertaken. For more information about the checks please see: Pre Employment Screening - Security Watchdog, part of Capita plc.
- Yoti will collect in date British or Irish passports should you choose to have your right to work in the UK check done online. Yoti will delete these details after 2 weeks and the details will then be stored on your employee file.
- We will provide MCL Medics (our Occupational Health provider) with your name, address, date of birth and telephone number and you will then be required to complete an on-line health questionnaire. You will also be required to undergo additional, regular occupational health assessments should your role requires this in line with the Health Surveillance programme. Please note that if your role is covered by the Health Surveillance programme these health assessments are mandatory.
- In line with the Rehabilitation of Offenders Act 1974 Act (as amended) applicants are asked at the application stage to disclose convictions which are defined as 'unspent' in terms of the Act, unless the nature of the role is that we are entitled to ask about an applicant's entire criminal record. Applicants are advised to read the University guidance and policy before completing the questions. More information is available in the University's Policy for Applicants with Declared Criminal Convictions: https://staff.napier.ac.uk/services/hr/HRDocuments/Pages/Policy%20A-Z.aspx
- During the recruitment process, applicants are invited to disclose protected characteristic information as defined in the Equality Act 2010 and other equalities related information. This information is anonymised and used for equality and statistical monitoring of applicants and employees.

How long is your information kept?

Unsuccessful applicants online accounts containing their information will be deleted 12 months after the last active account update. Applicant data processed on other University systems will be destroyed 12 months after the current academic year in which the recruitment campaign is conducted. Incomplete applications will also be deleted 12 months after the last active online account update.

If necessary, we may keep your data for longer and for up to 3 years if it is required:

- To respond to any queries or complaints
- To show that we have treated your fairly
- For legal or regulatory reasons and cannot be deleted as per the normal retention period.

Applicants who are holders of Tier 2 and Tier 5 visas will have their information stored until UK Visas and Immigration carries out an audit or as otherwise provided for by Immigration legislation.

Successful applicants will have their details kept on file for six years after termination of contract as their information will move from the recruitment process to the employment management process. For more information please see the Staff Privacy Notice at: staff.napier.ac.uk/statements

Further information can be found online at:
https://staff.napier.ac.uk/services/governance-compliance/governance/records/Pages/RecordsRetentionSchedules.aspx

How secure is your information?

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.

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.

Who keeps your information updated?

In order for us to keep your information up to date, we require you to inform us of any changes in the information you provide. You can also make changes to your online account yourself.

Will your information be used for any automated decision making or profiling?

No.

Is information transferred to a third country? Outside the UK/EEA and not included in the adequate countries list.

Yes. Capita PLC Security Watchdog may use processors outside the UK to process information. They use appropriate safeguards as required by Data Protection legislation. Please see their Privacy Notice for more information – link provided above.

Is any other information available?

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