**Edinburgh Napier University**
**Subject Access Request Procedure**

## 1. Statement

1.1. The University is the controller in relation to the processing of personal data in the course of its business activities.
1.2. All Data Subjects have the right of access to their own personal data. This document sets out the procedure to be followed in relation to any requests made for the disclosure of personal data processed by the University.

## 2. Definition of data protection terms

2.1. **Data Subjects** for the purpose of this procedure include all living individuals about whom we hold personal data, not only UK/EU citizens. This includes students, employees, 'workforce' and other stakeholders and individuals. All data subjects have legal rights in relation to their personal information.
2.2. **Personal data** means any information relating to an identified or identifiable natural person (a 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.
2.3. **Controllers** are the organisations (and those employed directly and indirectly by it to process personal data on its behalf) which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing policies and procedures in line with Data Protection law. We are the data controller of all personal data used in our business for our own commercial purposes and those for carried out as required by our Statutory Instruments (#557 of 1993, S76).
2.4. **Processing** is any activity that involves the use of the data. It includes obtaining, recording or holding data, or carrying out any operation or set of operations on the data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
2.5. **Workforce** includes, any individual employed by the University including staff/employees, contractors, agency staff, etc.

## 3. Recognising a subject access request

3.1. As the University processes personal data concerning data subjects, those data subjects have the right to access that personal data under Data Protection legislation.
3.2. A data subject is generally only entitled to access their own personal data, and not to information relating to other people.
3.3. A request to access personal data is known as a subject access request or SAR. Requests can be made either verbally or in writing. Where a request is made verbally we require this to be confirmed with a written request.

3.4. A SAR is a request by an individual to have a copy of their personal data, where this is not a routine request e.g. copy transcript dealt with by the Student Records Shop, although those requests are also subject to the legislation. SARs can be 'hidden' in other correspondence, such as complaints.
3.5. If any member of the University's 'workforce' received a SAR they must inform the Information Governance team (Governance Services) ***immediately*** (dataprotection@napier.ac.uk), in order for the response to be made within the legislative deadline.
3.6. A SAR will be considered and responded to in accordance with the Data Protection legislation.
3.7. Where a member of staff is unsure if they have received a SAR they should seek guidance from Governance Services/IG team (dataprotection@napier.ac.uk)

## 4. Verifying the identity of a Requester

4.1. The University is entitled to request additional information from a requestor in order to verify their identity and ensure the request is legitimate.
4.2. Where an individual is making a request for the personal data of a child the University will verify that the requestor has parental responsibility.
4.3. Where the University has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of two of the following:
  4.3.1. Current passport
  4.3.2. Current driving licence
  4.3.3. Recent utility bill with current address
  4.3.4. Birth/marriage certificate
  4.3.5. University ID card
  4.3.6. Evidence of parental responsibility (where appropriate)
4.4. If the University is not satisfied as to the identity of the requestor then the request will not be complied with, so as to avoid the potential for an inadvertent disclosure of personal data resulting in a data breach.
4.5. Staff will take particular care to verify the identity of the requestor where the request is received by email.

## 5. Fee for responding to requests

5.1. The University will usually deal with a SAR free of charge.
5.2. Where a request is considered to be manifestly unfounded or excessive a fee may be requested. Alternatively the University may refuse to respond to the request. If a request is considered to be manifestly unfounded or unreasonable the University will inform the requestor why this is considered to be the case.
5.3. A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charges taking into account the administrative costs of providing the information.

## 6. Time for responding to a SAR

6.1. The University has one month to respond to a SAR. This will run from the later of:
  6.1.1. The day of the request
  6.1.2. The date when any additional identification or other information requested is received, or
  6.1.3. Payment of any required fee.
6.2. In circumstances where the University is in any reasonable doubt as to the identity of the requestor, this period will not commence unless and until sufficient information has been provided by the requestor as to their identity, and in the case of a third party requestor the written authorisation of the data subject has been received (see 8. Below)
6.3. The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature or the request. The Data Protection Officer must always be consulted in determining whether a request is sufficiently complex as to extend the response period.
6.4. Where a request is considered to be sufficiently complex as to require an extension of the period for response, the University will notify the requestor within one calendar month of receiving the request, together with the reasons as to why this is considered necessary.

## 7. Form of response

7.1. A requestor can request a response in a particular form. In particular where a request is made by electronic means, then, unless the requestor has stated otherwise, the information should be provided in a commonly readable electronic format.

## 8. Sharing information with Third Parties

8.1. Data Subjects can ask that their personal data is provided via another person, such as an appointed representative (in such cases written authorisation signed by the data subject confirming the personal data to be provided, along with proof of their identity must be provided).
8.2. The response will not be provided until the University is satisfied that the request is bona fide and has received the data subject's written authorisation and proof of both parties identity. The University should not approach the data subject directly in these cases, but inform the requestor of the requirements.
8.3. If the University is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with the third party.
8.4. Personal data belongs to the data subject, and in the case of the personal data of a child, regardless of their age, the rights in relation to that personal data are theirs and not those of their parents. Parents, in most cases, do not have automatic rights to the personal data of their child.

8.5. However, there are circumstances where a parent can request the personal data of their child without requiring the consent of the child. This will depend on the maturity of the child and whether the University is confident that the child can understand their rights. Generally where a child is under 12 years of age they are deemed not to be sufficiently mature as to understand their rights of access and a parent can request access to their personal data on their behalf.
8.6. In relation to a child 12 years of age or older, then provided that the University is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the University will require the written authorisation of the child before responding to the requestor, or provide the personal data directly to the child in accordance with the process above.
8.7. In all cases the University will consider the particular circumstances of the case, and the above are guidelines only.

## 9. Withholding information

9.1. There are circumstances where information can be withheld pursuant to a SAR. These are specific exemptions and requests will be considered on a case by case basis.
9.2. Where the information sought contains the personal data of third party data subjects then the University will:
9.2.1. Consider whether it is possible to redact information so that this does not identify those third parties, taking into account that it may be possible to identify third parties from remaining information;
9.2.2. If this is not possible, consider whether the consent of those third parties can be obtained, and;
9.2.3. If consent has been refused, or it is not considered appropriate to seek that consent, then to consider whether it would be reasonable in the circumstances to disclose the information relating to those parties. If it is not then the information may be withheld.
9.3. So far as possible, the University will inform the requestor of the reasons why any information has been withheld.
9.4. Where providing a copy of the information requested would involve disproportionate effort the University will inform the requestor, seeking further detail from the requestor as to what they are seeking.
9.5. In certain circumstances information can be withheld from the requestor, including a data subject, on the basis that it would cause serious harm to the data subject or another individual. If there are any concerns in this regard then the Data Protection Officer will be consulted.

## 10. Process for dealing with a subject access request

10.1. When a SAR is received the Unviersity will:
10.1.1. Notify the IG team at dataprotection@napier.ac.uk who will be responsible for managing the response and consulting the Data Protection Officer if necessary;
10.1.2. The IG team will acknowledge receipt of the request within 5 days;

10.1.3. Take all reasonable and proportionate steps to identify and disclose the data relating to the request, this may include an electronic search using the full name of the data subject to ensure the search being conducted is appropriate and requesting information directly from University employees;

10.1.4. Never delete information relating to a SAR, unless it is deleted in the ordinary course of events, prior to being identified as pertaining to the request – it is an offence to amend or delete data following receipt of a SAR that would not have otherwise been so amended or deleted;

10.1.5. Consider whether to seek consent from any thirs parties which might be identifiable from the data being disclosed;

10.1.6. Seek legal advice, where necessary, to determine whether the University is required to comply with the request or supply the information sought;

10.1.7. Provide a written response, including an explanation of the types of data provided and whether and as far as possible for what reasons any data has been withheld; and,

10.1.8. Ensure that information disclosed is clear and technical terms are clarified and explained.